WebCCTV User's Manual

WebCCTV

Let's make things safer

1 Contents

1 CONTENTS 2

2 PREFACE 6

3 INTRODUCTION 13

4 GETTING STARTED 15

4.1 ACCESS WEBCCTV VIA INTERNET EXPLORER 15
4.2 ACCESS WEBCCTV LOCALLY 16
4.3 ADD WEBCCTV AS TRUSTED SITE 18
4.4 ADD WEBCCTV AS DEFAULT HOMEPAGE 20

5 VIDEO MANAGER 21

5.1 VIDEO MANAGER CONTROL PANEL 21
5.2 USERS 22
5.2.1 General Information 22
5.2.1.1 The Operator/User Account 23
5.2.1.2 The Administrator Account 23
5.2.2 Users - Add New User 24
5.2.3 Change Your Password 25
5.2.4 User Actions Log 25
5.2.4.1 Log Search 26
5.2.4.2 Event Logger Configuration 27
5.2.5 Connected Users 28
5.3 SETTINGS 29
5.3.1 Cameras 30
5.3.1.1 Camera Wizard 31
5.3.1.1.1 Name & Type 32
5.3.1.1.2 Connection 33
5.3.1.1.3 Live View 35
5.3.1.1.4 Recordings 37
5.3.1.1.5 Activity 38
5.3.1.1.6 PTZ 41
5.3.1.1.7 Virtual Patrol 42
5.3.1.1.8 Users 44
5.3.1.2 Network Video Server Wizard 45
5.3.1.2.1 Name & Type 46
5.3.1.2.2 Connection 47
5.3.1.2.3 Video Settings 48
5.3.1.2.4 Name 49
5.3.1.2.5 Recordings 50
5.3.1.2.6 Activity 51
5.3.1.2.7 PTZ 54
5.3.1.2.8 Virtual Patrol 55
5.3.1.2.9 Users 57
5.3.2 Alarms 58
5.3.2.1 Picolo I/O Proxy 59
5.3.2.1.1 Name 60
5.3.2.1.2 Configuration 61
5.3.2.1.3 Outputs 62
5.3.2.2 PMD I/O Device 63
5.3.2.2.1 Name 64
5.3.2.2.2 Configuration 65
5.3.2.2.3 Outputs 67
5.3.2.2.4 Delete PMD I/O Device 68
5.3.2.2.5 PMD I/O serial number 69
5.3.2.3 Generic Alarm Driver 70
5.3.2.3.1 Name 71
5.3.2.3.2 Protocol 72
5.3.2.3.3 Connection 72

5.3.2.4 RedLight Alarm Driver 73
5.3.2.4.1 Name 74
5.3.2.4.2 Protocol 75
5.3.2.4.3 Connection 76
5.3.2.5 Alarm Configuration Wizard 77
5.3.2.5.1 Name 78
5.3.2.5.2 PTZ 79
5.3.2.5.3 Recordings 80
5.3.2.5.4 FTP 81
5.3.2.5.5 Outputs 82
5.3.2.5.6 Notification 83
5.3.2.5.7 Mail 84
5.3.2.5.8 SMS 85
5.3.3 POS 86
5.3.3.1 Serial Port POS 88
5.3.3.1.1 Remote POS Monitor 89
5.3.3.1.2 Name 93
5.3.3.1.3 Protocol 94
5.3.3.1.4 Connection 94
5.3.3.1.5 Storage 94
5.3.3.1.6 Name 95
5.3.3.1.7 Recordings 96
5.3.3.2 Generic POS 97
5.3.3.2.1 Name 98
5.3.3.2.2 Protocol 99
5.3.3.2.3 Connection 99
5.3.3.2.4 Storage 99
5.3.3.2.5 Name 100
5.3.3.2.6 Recordings 101
5.3.3.3 TP.Net 102
5.3.3.3.1 Name 103
5.3.3.3.2 Protocol 104
5.3.3.3.3 Connection 105
5.3.3.3.4 Storage 105
5.3.3.3.5 Name 106
5.3.3.3.6 Recordings 107
5.3.3.4 NAMOS 108
5.3.3.4.1 Name 109
5.3.3.4.2 Protocol 110
5.3.3.4.3 Connection 110
5.3.3.4.4 Storage 110
5.3.3.4.5 Name 111
5.3.3.4.6 Recordings 112
5.3.4 Storage Manager 113
5.3.4.1 Adding, configuring & deleting a Volume 113
5.3.4.1.1 Location 114
5.3.4.1.2 Cameras 116
5.3.4.1.3 Storage Parameters 117
5.3.4.2 Advanced Storage Settings 119
5.3.4.2.1 Movie Lifetime 119
5.3.4.2.2 Alarms 120
5.3.4.2.3 POS 121
5.3.4.3 Detailed Storage Information 122
5.3.5 Single View 123
5.3.5.1 Frame rate 124
5.3.5.2 Sequence 125
5.3.6 Mosaics 127
5.3.7 Network Settings 129
5.3.7.1 Network settings 130
5.3.7.2 FTP Parameters 130
5.3.7.3 SMS Account Parameters 131
5.3.7.4 E-Mail Profile 132

5.3.8 Certificate Management *134*
5.3.8.1 Self-signed certificates 135
5.3.8.2 CA signed certificates 136
5.4 INFO 137
5.4.1 System Info *138*
5.4.1.1 System Configuration 139
5.4.1.1.1 Saving Configuration 139
5.4.1.1.2 Restoring Configuration 139
5.4.1.2 System Information 141
5.4.2 Network Diagnostics *142*
5.4.2.1 Port Scanning 143
5.4.2.2 Camera Scanning 143
5.4.3 Server Messages Log *144*
5.4.3.1 Log Search 144
5.4.3.2 Event Logger Configuration 146
5.4.4 System Downloads *147*
6 VIDEO BROWSER 148
6.1 VIDEO BROWSER CONTROL PANEL 148
6.2 LIVE 149
6.2.1 Single View *151*
6.2.1.1 Sequences 152
6.2.1.2 Mosaics 152
6.2.1.3 Changing Video Window Size 152
6.2.1.4 Low/High Bandwidth Mode 152
6.2.1.5 Snapshots 153
6.2.1.6 PTZ 153
6.2.1.7 Digital Zoom 154
6.2.1.8 Audio 154
6.2.2 Mosaic View *157*
6.2.2.1 Sequences 158
6.2.2.2 Mosaics 158
6.2.2.3 Changing Video Window Size 158
6.3 RECORDINGS 159
6.3.1 Select Time Period *160*
6.3.2 Single Playback *161*
6.3.2.1 Single Playback Controls 163
6.3.2.2 Switching sources 163
6.3.2.3 Activity Level 163
6.3.2.4 Slider 163
6.3.2.5 Changing Video Window Size 163
6.3.2.6 Low/High Bandwidth Mode 163
6.3.2.7 Snapshots 164
6.3.2.8 Digital Zoom 164
6.3.3 Synchronized Playback *165*
6.3.3.1 Synchronized Playback Controls 166
6.3.3.2 Switching sources 166
6.3.3.3 Slider 166
6.3.3.4 Changing Video Window Size 166
6.3.4 Alarms *167*
6.3.5 POS *168*
6.3.6 Movie Export *169*
6.3.6.1 Creating Export 170
6.3.6.2 Saving Export Files to Hard Disk 170
6.3.6.3 Saving Export Files to CD 171
6.3.6.4 Checking Digital Signature 173
6.4 ALARMS 181
6.4.1 View Alarm Movie *182*
6.4.2 Export Alarm Movie *182*
6.4.3 Slider *182*
6.4.4 Alarm Playback Controls *183*
6.4.5 Changing Video Window Size *183*

6.4.6 Low/High Bandwidth Mode *183*
6.4.7 Snapshots *183*
6.4.8 Digital Zoom *184*
6.5 POS 185
6.5.1 View POS Movie and Ticket *186*
6.5.2 Export POS Movie *186*
6.5.3 Slider *186*
6.5.4 POS Playback Controls *187*
6.5.5 Changing Video Window Size *187*
6.5.6 Low/High Bandwidth Mode *187*
6.5.7 Snapshots *187*
6.5.8 Digital Zoom *188*
7 APPENDIX A 189
8 APPENDIX B 194
9 GLOSSARY 199

2 Preface

This document

This manual is intended for administrators and operators of a WebCCTV Video Recorder and is applicable for WebCCTV software version 4.0 and higher.

Safety Notices

Please observe all safety notes and instructions carefully when using this product.

Liability

The information in this publication is believed to be accurate in all respects. Quadrox assumes no responsibility for incidental or consequential damages incurred directly or indirectly from errors, omissions or discrepancies in connection with the furnishing, performance or use of this manual. The information contained herein is subject to change without notice. Revisions or new editions to this publication may be issued to incorporate such changes. All rights reserved. Under the copyright laws, no part of this manual can be reproduced in any form without written permission of Quadrox.

Legal considerations

Please check your local regional laws and regulations before using WebCCTV for surveillance purposes. Camera surveillance maybe prohibited by laws, which may vary from country to country.

Trademark Acknowledgments

Quadrox, WebCCTV, Internet Explorer, Windows are registered trademarks of the respective holders.

Support Services

Should you require any technical assistance, please contact your installer. If your questions cannot be answered immediately, your installer will forward your queries through the appropriate channels to ensure a fast response.

License Agreement

Copyright (C) 1997-2008 by Quadrox tsov. All rights reserved.

PLEASE, READ THIS DOCUMENT CAREFULLY BEFORE INSTALLING THE SOFTWARE. BY INSTALLING AND USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THE AGREEMENT, DO NOT INSTALL OR USE THE SOFTWARE.

SOFTWARE LICENSE AGREEMENT

This Software License Agreement ("SLA") is a legal agreement between you ("Customer," either an individual or an entity) and Quadrox tsov ("Quadrox"). The term "Software" as used in this SLA means the computer software contained in the package or file(s) to which this SLA is annexed, the associated media, any printed documentation and materials, and any "on-line" or electronic documentation provided by Quadrox related to such software. By opening the packaging, downloading, indicating your acceptance on-screen or on-line, or installing and/or using the Software, you are agreeing to be bound by the terms of this SLA.

If you do not agree to the terms of this SLA,

(a) you may not use the Software,

(b) if you have received physical copies of the Software from Quadrox, you must promptly return the uninstalled Software, and all accompanying items as defined above, to Quadrox within ten (10) days of your receipt, in exchange for which you will receive a full refund of any paid license fees, and

(c) you must immediately remove from your systems and destroy any and all copies of the Software and all of its component parts.

1. CONTROLLING LANGUAGE

The controlling language of this SLA will be English. Quadrox has provided translations in Dutch, French, German, Spanish Italian, Russian and other languages solely for the convenience of the Customer.

2. GRANT OF LICENSE

Subject to the terms and conditions of this SLA, Quadrox hereby grants you a nonexclusive, non-transferable license ("Software License") to use the enclosed Software within the Territory, in the operating environment identified by Quadrox, either

(a) to the extent specified in an authorization certificate distributed to Customer by Quadrox, or

(b) if not specified, for a single user on a single computer.

For purposes hereof, "Territory" means, for a "U.S. Version" the United States and Canada, and for the "International Version" all countries except those countries where

exportation or transmission is prohibited by any applicable EU, U.S. or other law or regulation, or in which any provision of this SLA is not enforceable Customer represents that it has complied with any regulations or registration procedures required by applicable law to make this license enforceable. This SLA does not grant you any rights in connection with any trademarks or service marks of Quadrox. The license granted herein is conditional on timely payment in full of all applicable invoices and charges. Maintenance for the Software is subject to separate charges and is governed by Quadrox's standard maintenance policy, which policy is available from Quadrox in written form and is subject to change from time to time.

3. TRIAL VERSIONS

If the Software was provided to you on a no-charge basis pursuant to a Quadrox trial program (a "Trial Version"), then, in addition to the other provisions and limitations hereof,

(a) the Software may be used solely for evaluation purposes for the period specified by Quadrox at the time of delivery, and if no such period has been specified, then for a period of thirteen (30) days (the "Trial Period"), and

(b) the Software may not be used for any development, commercial, or production purpose.

Further, in the event you have acquired a Trial Version, you must purchase a full-use license

(i) if you wish to use the Software after the end of the Trial Period, or

(ii) if you wish to use the Software for any development, commercial, or production purpose.

If at the end of the Trial Period you do not purchase a full-use license, you must destroy any and all copies of the Software and all of its component parts.

4. RESTRICTIONS ON USE

You may use the Software solely for your own internal data processing operations. You may make one copy of each licensed Software item (other than Trial Version Software) for backup purposes only. No other copies shall be made without Quadrox's prior written consent. If the Software is an upgrade of a previous version of the product, you may now use that upgraded product only in accordance with this SLA (provided you discontinue the use of the un-upgraded version).

You shall not:

(a) remove any product identification, copyright notices, or other notices or proprietary restrictions from the Software;

(b) make the Software available for commercial timesharing, rental, application service provider or service bureau use;

(c) except as provided in paragraph 6, transfer, sell, assign or otherwise convey the Software to another party without Quadrox's prior written consent;

(d) translate or otherwise prepare any derivative works based on the Software;

(e) disclose any information related to the Software, including without limitation diagnostic tests, screen images, printed output, or results of any performance or benchmark tests of any Software to any third party without Quadrox's prior written approval;

(f) use the Software as an aid to develop or market a competing product;

(g) make any attempt to bypass or disable product serialization or time limit mechanisms where such mechanisms are utilized in the Software's programming, or

(h) transfer or use the Software outside of the Territory without Quadrox's prior written consent and without paying any applicable additional fees.

You further agree to comply fully with all laws and regulations to assure that, should such consent be granted, neither the Software, nor any direct product thereof, is exported, directly or indirectly, in violation of law.

You also agree not to cause or permit the Software to be dumped, traced, disassembled, decompiled or otherwise reverse engineered except to the extent

(x) applicable law expressly requires that you be permitted to decompile,

(y) it is essential to do so in order to achieve interoperability of the Software with another software program, and

(z) you have first requested Quadrox to provide the information necessary to achieve such interoperability and Quadrox has not made such information available in accordance herewith.

Quadrox has the right to impose reasonable conditions and to request a reasonable fee before providing such information. Any information supplied by Quadrox or obtained by you, as permitted hereunder, may only be used by you for the purpose described herein and may not be disclosed to any third party or used to create any software which is substantially similar to or competitive with the Software.

5. COPYRIGHT/OWNERSHIP OF SOFTWARE

The Software is the proprietary product of Quadrox or its suppliers and is protected by copyright, trade secret, patent and other intellectual property laws and international treaties. You acquire only the right to use the Software and do not acquire any rights, express or implied, in the Software or media containing the Software other than those specified in this SLA. Quadrox or its suppliers shall at all times retain all rights, title, and interest, including intellectual property rights, in the Software and its media. You agree not to challenge the validity of Quadrox's or its suppliers' copyright or trademark rights in and to the Software.

6. TRANSFER OF LICENSE

This Software License may not be transferred to a replacement computer or transferee of the original licensed computer without Quadrox's prior written permission and the payment of applicable fees. If such permission is granted by Quadrox, you may transfer the Software

License to a replacement computer or to the transferee of the originally licensed computer, provided, that any such transferee agrees to and accepts all the terms of this SLA and you do not keep any portion or copy of the Software and all accompanying items (including any documentation, binders or other printed materials). You may not under any circumstances carry out any transfer permitted by the foregoing by means of communication over the Internet or any other public network.

7. LIMITED WARRANTIES/EXCLUSIVE REMEDIES

Quadrox warrants that for 30 days from date of delivery to you:

(a) enclosed media (if any) is free of defects in materials and workmanship under normal use; and

(b) unmodified Software will substantially perform the functions described in documentation provided by Quadrox when operated on the designated computer and operating system. Quadrox and its suppliers do not warrant that:

(i) the Software will meet your requirements,

(ii) the Software will operate in combinations you may select for use,

(iii) operation of the Software will be uninterrupted or error-free, or

(iv) all Software errors will be corrected.

THESE WARRANTIES ARE EXCLUSIVE AND IN LIEU OF ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

If you report an error in the Software within the 30 day period, Quadrox shall, at its option, correct the error, provide you with a reasonable procedure to circumvent the error, or, upon return of the Software to Quadrox, refund the license fees. Quadrox will replace any defective media without charge if it is returned to Quadrox within the 30 day period. These are your sole and exclusive remedies for any breach of warranty. This limited warranty gives you specific legal rights. You may have others, which may vary from place to place based on local laws, if applicable. You further acknowledge your understanding that if the Software is a Trial Version, Quadrox does not make any commitment to you to provide any support. In any event, Quadrox reserves the right to cease support of the Software and to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or other characteristics of the Software.

EXCEPT FOR THE LIMITED WARRANTIES DESCRIBED ABOVE, THE SOFTWARE IS PROVIDED "AS IS", AND TO THE FULLEST EXTENT PERMITTED BY LAW, QUADROX AND ITS SUPPLIERS DISCLAIM ANY AND ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND/OR FITNESS FOR A PARTICULAR PURPOSE. YOU, THE END USER, ASSUME THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE SOFTWARE.

8. LIMITATION OF LIABILITY

QUADROX AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY CUSTOMER OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. QUADROX'S AND ITS SUPPLIERS' LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED THE FEES PAID BY CUSTOMER FOR THIS LICENSE. IF A COURT OR ARBITRATION TRIBUNAL (AS APPROPRIATE HEREUNDER) DETERMINES THAT ANY REMEDY PROVIDED TO YOU UNDER THIS SLA HAS FAILED OF ITS ESSENTIAL PURPOSE, THE LIMITATIONS ON LIABILITY AND EXCLUSION OF DAMAGES ABOVE SHALL NOT BE AFFECTED AND SHALL REMAIN IN FULL FORCE AND EFFECT.

9. BINDING AGREEMENT

This SLA is a legally binding agreement between you and Quadrox and it is the complete and exclusive statement of all the terms which gives you the right to use the Software. No other terms, including, without limitation, those contained in any purchase orders or other forms shall be of any force or effect and only the terms of this SLA shall govern for all purposes; provided, that if you have previously executed (and Quadrox has accepted) a Quadrox Order Form, or if Quadrox has previously accepted your purchase order, or if there was previously a Quadrox license agreement in effect regarding the Software (each, a "Prior Agreement"), this SLA shall be deemed to modify and amend the Prior Agreement with regard to the subject matter covered by this SLA (and your acceptance of the terms of this SLA shall serve as an expression of your agreement to such modification), provided further, that any obligation to pay fees arising under the Prior Agreement shall survive. In the event of any termination of the license grant herein, the provisions of paragraphs 1 and 3 through 13 hereof shall continue in full force and effect.

Without prejudice to any other rights, Quadrox may terminate this SLA if you fail to comply with any of its terms and conditions. In such event, you must destroy any and all copies of the Software and all of its component parts.

10. RESTRICTED RIGHTS

The Software is provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the U.S. Government is subject to restrictions as currently set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252-227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227.19, as applicable.
Manufacturer is Quadrox tsov vul. Heroiv Kosmosu 4, 8th floor, 03 148 Kyiv, Ukraine.

11. SEVERABILITY

If any provision, or portion thereof, of this SLA is invalid under any applicable statute or rule of law, it is to that extent to be deemed omitted.

12. APPLICATION

EUROPEAN UNION GOVERNMENT RESTRICTED RIGHTS

All Software and related documentation are provided with restricted rights. Use, duplication or disclosure by the EU Government is subject to legal restrictions. If you are sub-licensing or using the Software outside of the EU, you will comply with the applicable local laws of your country, EU export control law, and the English version of this Agreement.

MANUFACTURER

The Manufacturer for the Software is:

Quadrox tsov.
Raisy Okypnoi 4a
Office 71
02002 Kyiv
Ukraine

GENERAL

This Agreement is binding on you as well as your employees, employers, contractors and agents, and on any successors and assignees. Neither the Software nor any information derived there from may be exported except in accordance with the laws of the EU or other applicable provisions. This Agreement is governed by the laws of the European Union (except to the extent local law governs copyrights and locally registered trademarks). This Agreement is the entire agreement between us and supersedes any other understandings or agreements, including, but not limited to, advertising, with respect to the Software. If any provision of this Agreement is deemed invalid or unenforceable by any country or government agency having jurisdiction, that particular provision will be deemed modified to the extent necessary to make the provision valid and enforceable, and the remaining provisions will remain in full force and effect.

For questions concerning this Agreement, product or technical matters, please contact Quadrox tsov at the address stated above.

3 Introduction

WebCCTV is a unique digital video surveillance solution, which combines three major functions in one Network Video Recorder (NVR) or Digital Video Recorder (DVR): local digital recording, multiplexing and simultaneous transmission of the video via existing networks (TCP/IP). To a standard WebCCTV, up to 16 cameras can be permanently recorded while multiple operators at different locations on the network are accessing the WebCCTV device.

Being a networked device, WebCCTV utilizes two basic principles of the Internet/Intranet technology:

- WebCCTV works over the TCP/IP network protocol, which provides maximum connectivity. This means that the existing computer network infrastructure can be used eliminating extra installation expenses.
- WebCCTV uses a web-based user interface to view live images, recordings, etc. More specific it uses Microsoft **Internet Explorer.**

Remote and Local Monitoring

To remotely monitor the connected cameras, the WebCCTV uses Web Browser technology. To locally monitor video, the WebCCTV also provides a local interface via a PC monitor directly connected to the WebCCTV. This local interface allows an operator to see live video from the connected cameras without the need for additional client computers on a network.

Continuous Activity-Based Recording

By default, a WebCCTV continuously records all images from all the connected cameras based on activity detection. In this case, only movement is recorded. If there is no movement, no recording takes place. If necessary, the WebCCTV can be set to record continuously.

Intelligent Storage Option

WebCCTV uses a first-in/first-out (FIFO) overwrite principle. Once the disk is full, the oldest images are overwritten.

Semi-Continuous recording (recording based on activity detection) allows a WebCCTV to store pre- and post-alarm video. Pre- and Post-alarm images are often more important than the images at the time of the alarm event itself. Up to 5 minutes of pre- and post-alarm video can be stored.

WebCCTV makes a distinction between common activity recordings and pre/post alarm recordings. In the way that, alarm recordings have a higher storage priority and will not be overwritten by non-alarm recordings.

The WebCCTV is operational even when no live monitoring occurs. While the WebCCTV continuously records images from all the cameras, video is transmitted from the server to the client **only** when an Internet browser is connected to WebCCTV and someone is live-viewing images from one or more cameras.

4 Getting Started

This chapter provides information to get you started using your WebCCTV. It covers the following topics:

- Accessing WebCCTV via Internet Explorer.
- Accessing WebCCTV locally.
- Setting up WebCCTV application as default homepage.
- Add WebCCTV as a trusted site.

4.1 Access WebCCTV via Internet Explorer

WebCCTV automatically starts recording the moment it is turned on and booted. The booting process takes about two minutes.

The WebCCTV can be accessed via Internet Explorer. This Internet Explorer browser can reside on three places:

1. A capable client LAN PC: This is a PC in the same network as the WebCCTV
2. A capable client WAN PC: This is a PC on the wide area network. Your router/firewall has to be configured properly in order to connect to WebCCTV.
3. The WebCCTV: On the desktop of the WebCCTV, you can click the video browser icon which will open the Internet Explorer browser on the WebCCTV itself automatically redirecting you to the WebCCTV server.

Only 'ActiveX' supporting Internet Browsers are designed to be used with the WebCCTV. Internet browsers like Netscape, Opera and other browsers that do not support 'ActiveX', are not suitable for use with WebCCTV.

To access the WebCCTV server via Internet Explorer, follow the steps below:

1. Obtain the exact IP address for the WebCCTV from your System Administrator and make note of it for future reference.

'http://192.168.100.1/' is the factory default IP-address for a WebCCTV. Please note that your installer could have changed it to fit the specifications of your own network.

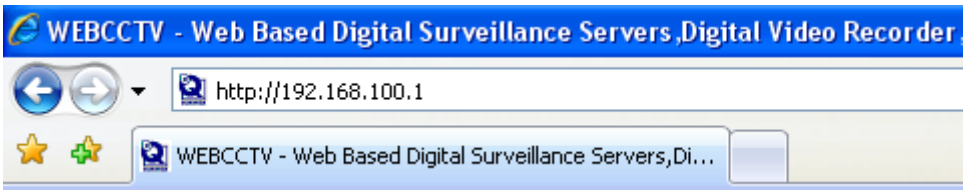
2. Open Internet Explorer.

Click the **Start** button on your PC or WebCCTV and find **Internet Explorer** in the **All Programs** tab. An Internet Explorer link can often be found on the desktop.

3. Once Internet Explorer is opened, click on the address field and enter the IP-address as shown in the example below:

   http://192.168.100.1/

Make sure to include the **http** prefix into the IP-address. This is a protocol used for communication with a World Wide Web server. Since WebCCTV uses the same technology, the http prefix should be included.


WEBCCTV - Web Based Digital Surveillance Servers,Digital Video Recorder
http://192.168.100.1
WEBCCTV - Web Based Digital Surveillance Servers,Di...

WebCCTV IP-address

When you changed the TCP/IP communication port, you need to add the port in the IP-address. For example, if you changed the TCP/IP port to 81 (80 is default port), the IP-address becomes 'http://192.168.100.1:81/'.

If you want to connect to a GuardNVR or GuardDVR, your IP-address becomes 'http://192.168.100.1/guardnvr' or 'http://192.168.100.1/guarddvr'

If the WebCCTV is accessed for the first time with a client PC, you will need to install the ActiveX component. Follow the instructions on your screen.

Installation of the component is done (semi) automatically on the first connection to a WebCCTV. The installation only has to be done once.

4.2 Access WebCCTV locally

The WebCCTV Local User Interface allows you to view video footage in real time by connecting a monitor directly to WebCCTV while recording at the same time.

Compared to Internet Explorer access, accessing WebCCTV via the Local Interface has limited user functionality. The Local Interface access does not consume much CPU and memory. Accessing WebCCTV via Local Interface slightly increases image quality.

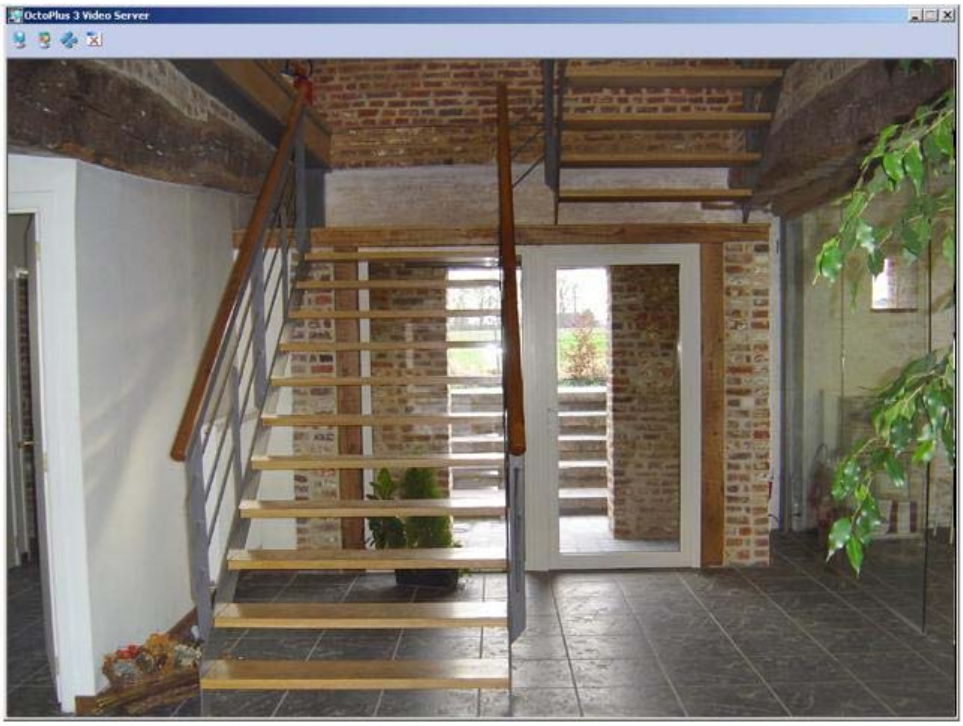
To access WebCCTV locally, please follow the steps below:

1. Connect a monitor, a keyboard and a mouse directly to the WebCCTV.
2. By default, a standard Windows Login window will appear on the screen. Login with administrative credentials.

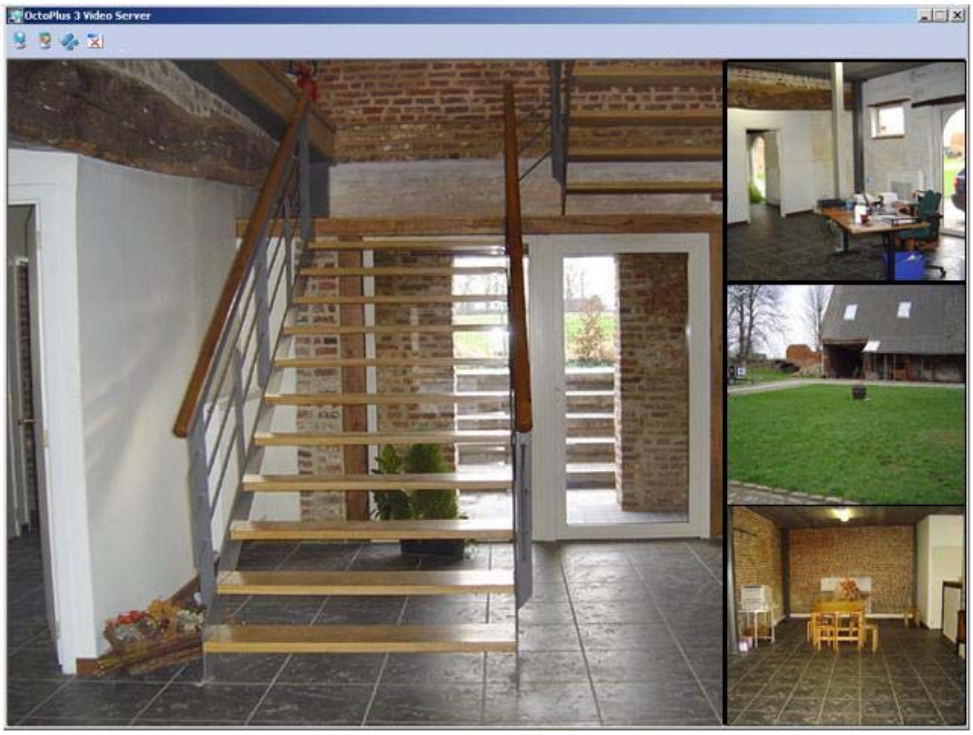
Please contact your installer for the correct details.

3. Depending on how you accessed the WebCCTV last time, you will see either a WebCCTV Local Interface directly on the screen or a WebCCTV Local Interface icon on the system tray in the right bottom corner.
4. Double click the Local Interface icon to restore the Local Interface.

It's possible to configure the WebCCTV not to show the Windows logon screen after a restart and go directly to the Local Interface. To achieve this double-click the icon "Operator Mode" on the WebCCTV desktop.



WebCCTV Local Interface Single View Screen



WebCCTV Local Interface Mosaic View Screen

WebCCTV Local Interface Control Panel

WebCCTV Local Interface provides basic Live view functionality (in Single or Mosaic View). For complete WebCCTV functionality including settings, recordings, exporting, etc., access the WebCCTV server via Internet Explorer.

WebCCTV Local Interface Buttons

Single View

Click on this button to access live view from a single camera.

Mosaic View

Click on this button to live view multiple cameras.

Full Screen Button

Click on this button to extend the application window to full screen view.

Close Child Windows Button

Click on this button to close all the windows on the screen

Change Mosaic View Button

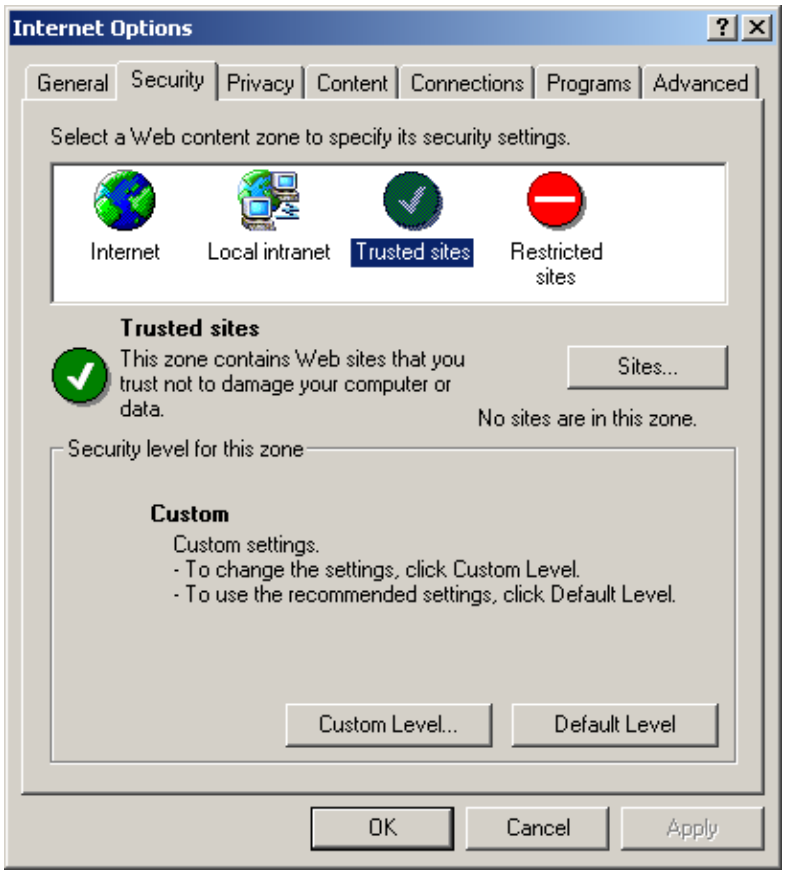
This button is applicable only if more than 4 cameras are connected; it allows you to jump from one mosaic view to another.

4.3 Add WebCCTV as trusted site

The trusted sites zone contains sites you trust; sites that you believe you can download or run files from without worrying about damage to your computer or data. The default security level for the trusted sites zone is Low, therefore, Internet Explorer will allow all cookies and ActiveX controls from Web sites in this zone to be saved on your computer and read by the Web site that created them. We recommend adding WebCCTV to the trusted sites zone.

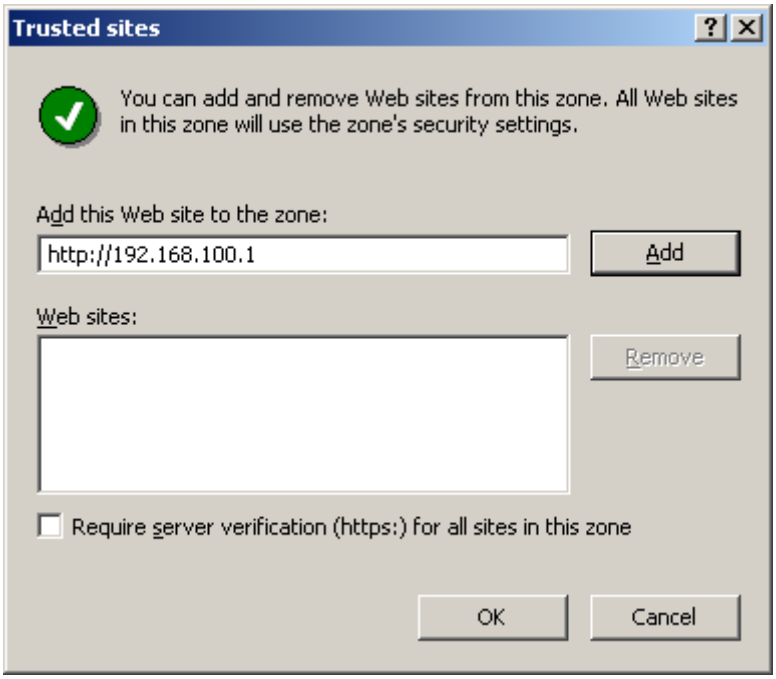
To add the WebCCTV application as a trusted site, follow the steps below:

1. Select **Tools** on the Internet Explorer menu bar.
2. Select **Internet Options**.
3. Go to the **Security** tab. Select **Trusted Sites** there.



Internet Options Screen

4. Click the **Sites** button. In the window that appears deselect **Require server verification (https:) for all sites in this zone** check box.


Trusted sites
You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.
Add this Web site to the zone:
http://192.168.100.1
Add
Web sites:
Remove
Require server verification (https:) for all sites in this zone
OK
Cancel

Trusted Sites Screen

5. Specify the correct WebCCTV server address in the corresponding field and click the **Add** button.
6. The address you specified appears in the **Web sites** filed.
7. Click **OK.**

4.4 Add WebCCTV as default homepage

To make WebCCTV a default start page on a client PC, follow the steps below:

1. Select **Tools** on the Internet Explorer menu bar.
2. Select **Internet Options**.
3. Select **General**.
4. Click **Use Current** button or enter **http://192.168.100.1** IP-address (or the correct WebCCTV IP-address) as your new default homepage.

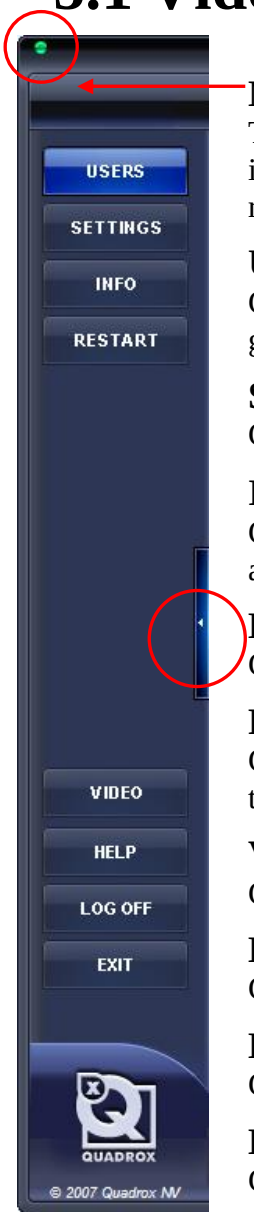
5 Video Manager

To log on to the Video Manager application, you need administrative rights.

This chapter provides an overview of the WebCCTV Video Manager Control Panel and the following WebCCTV functions:

- Users
- Server Settings
- General Server Information

5.1 Video Manager Control Panel



Network status indicator
The green dot, in the top left corner, indicates a good network status. When the indicator is red, the WebCCTV is experiencing network problems which can result in slow response from the Web Application, or no response at all.

Users
Click this button to access the Users screens where you can add or delete users, give different user rights, check Connected Users and User Actions logs.

Settings
Click this button to change the WebCCTV settings to your requirements.

Info
Click this button to see general server information. This section also provides access to Network Diagnostics, System Downloads and the Server logs.

Hide Control Panel
Click this button to hide or retrieve the control panel.

Restart
Click this button to restart the video server. Usually there's no need to restart the server unless the Restart button becomes red.

Video
Click this button to open the Video Browser application.

Help
Click this button to access WebCCTV Online help.

Log Off
Click this button to change user.

Exit
Click this button to exit the WebCCTV application.

5.2 Users

This chapter provides an overview of the Users section of WebCCTV**.**

5.2.1 General Information

WebCCTV is a multi user system capable of supporting an unlimited number of users. Every registered user can have the following properties and user rights:

Property	Description	Limitation
Name	Is used for the identification of the user	Must be unique
Password	Password related to the user for login	No limitation
Language	Preferable language for the user	English, Dutch, French, Italian, German, Spanish, Russian, Ukrainian

User Rights	Description
Live	Access to live view
PTZ*	Access to PTZ controls
Recordings	Access to view the recorded video footage
Export	Access to the export menu
Alarms	Access to view alarms and related video footage
POS	Access to view POS transactions and related video footage
User management**	Access to change user privileges, view user actions log, view connected users
System configuration**	Access to modify system options
* setting presets are only available to users with administrator rights	
** only available to users with administrator rights	

Users with administrator rights can allow or block the viewing of certain cameras for non-administrative users.

By default WebCCTV has two user accounts:

- Operator Account
- Administrator Account

The default operator and administrator account can't be deleted.

WebCCTV Users management is fully integrated into the Windows Operating System users system, which results in very strong and safe access procedures.

5.2.1.1 The Operator/User Account

A non-administrative user can have different privileges and rights. He doesn't have access to the video manager application.

The default operator account can't be deleted.

5.2.1.2 The Administrator Account

A user with Administrator Rights can:

- Add new users
- Change passwords
- Delete users
- Set user privileges
- View User Actions Logs
- View Connected Users

The default administrator account can't be deleted.

A User name can't be changed once it has been added. It can only be deleted. The only parameters that can be changed are User Type, User Password, User Language and User privileges.

Only an Administrator can grant, limit and edit user rights.

The screen shown below is displayed when you click on the **Users** button.

Users Screen

All subsections of the users menu are:

- Users
- Change Your Password
- User Actions Log
- Connected Users

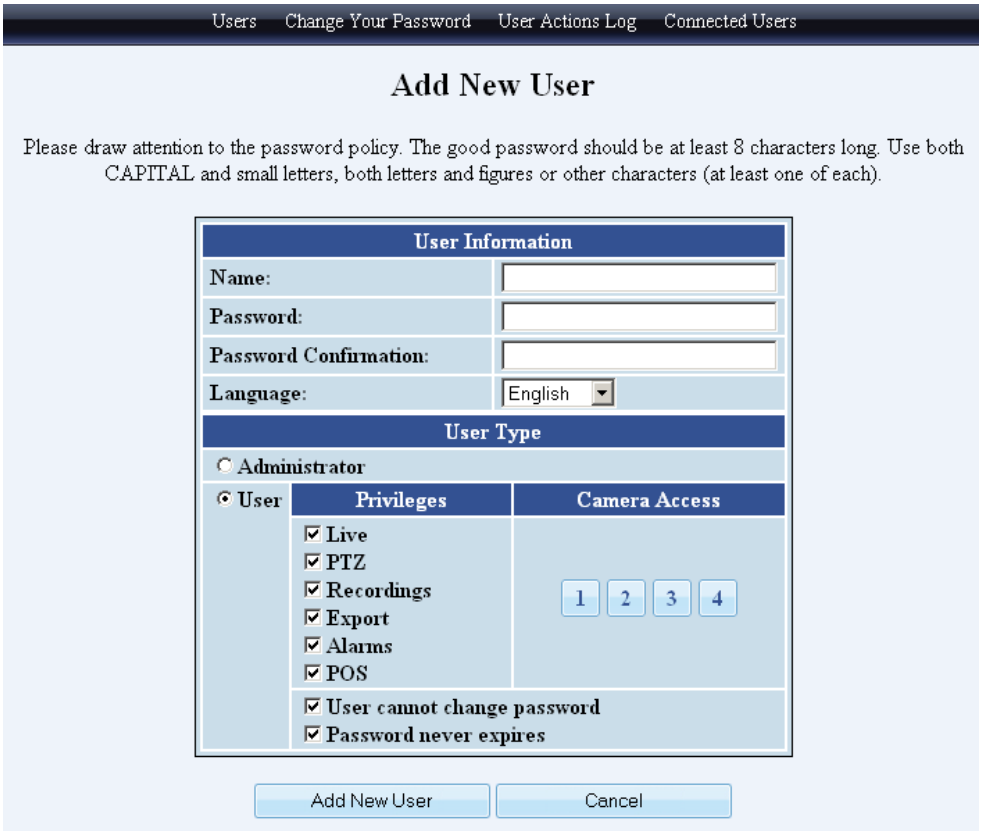
5.2.2 Users - Add New User

By clicking the Users button, you are automatically taken to the Users section. To add a new user to the WebCCTV, follow the steps below:

1. Click the **Add New User** button. The New User Window shown below will be displayed.
2. Enter a Name.
3. Enter a Password.
4. Confirm the Password.
5. Select the interface language for the new user.
6. Select the privileges for the new user.
7. Define which cameras the user should be able to view. By default, all cameras are enabled. Click a camera button to disable it. When disabled, a camera button is red, whereas an enabled camera button has the regular blue color.
8. Define the ability for a user to change his password by (de)selecting the **User cannot change password** check box.
9. Select the **Password never expires** check box if you don't want the password to expire. Otherwise a user will be forced to change the password every 6 weeks.

By default, a newly-added user has access to all the cameras.

10. Click **Add new user** to confirm the entered user data.



Add New User Screen

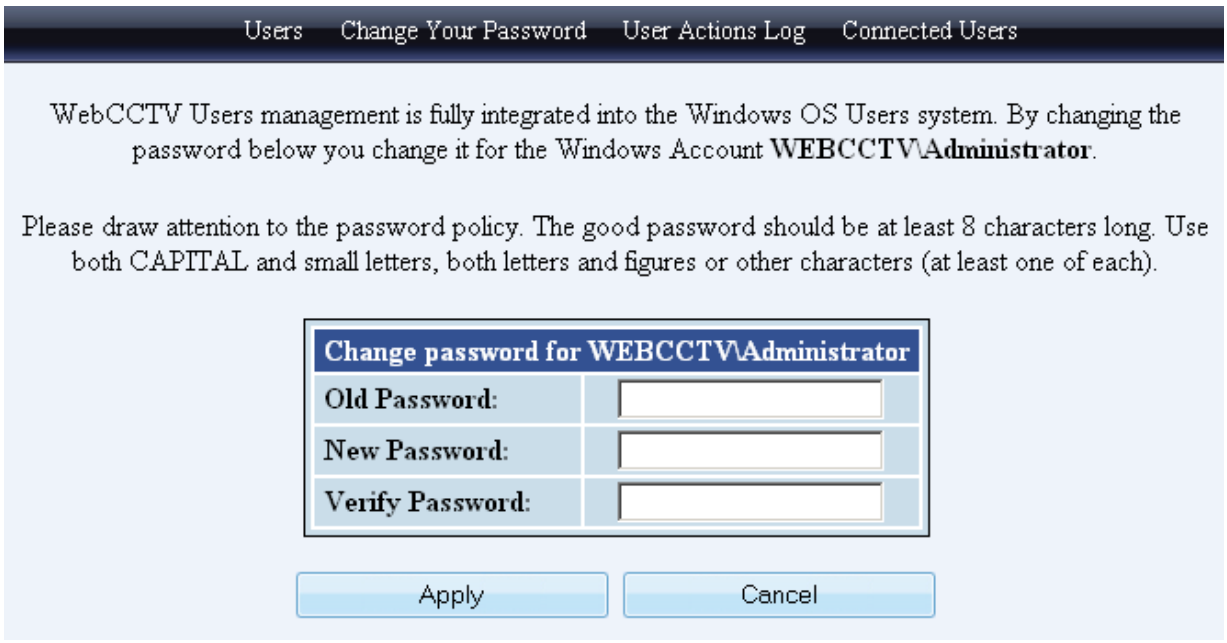
5.2.3 Change Your Password

Changing your password from time to time helps to protect your system from unauthorized access.

To change the password, follow the steps below:

1. Enter the old password.
2. Enter the new password.
3. Enter the password confirmation.
4. Click **Apply**. The new password should be set now.

WebCCTV has no specific minimum password length limitation. When choosing a password, try to take a password of at least 8 characters and use both capital and small letters, both letters and figures or other characters (at least one of each).


Users
Change Your Password
User Actions Log
Connected Users
WebCCTV Users management is fully integrated into the Windows OS Users system. By changing the password below you change it for the Windows Account WEBCCTV\Administrator.
Please draw attention to the password policy. The good password should be at least 8 characters long. Use both CAPITAL and small letters, both letters and figures or other characters (at least one of each).
Change password for WEBCCTV\Administrator
Old Password:
New Password:
Verify Password:
Apply
Cancel

Change Your Password Screen

Click on **Cancel** if you want to reset your form.

5.2.4 User Actions Log

WebCCTV stores all user actions in its User Actions Log. Example of user actions are live views, recording views, user management changes, etc. This log is kept inside the Windows operating system itself. Technically, it is kept inside a specific WebCCTV event log container in the Windows event logging subsystem.

The amount of logged user actions (number of days contained in the log) depends on the defined size of the event viewer. In normal circumstances, the log is large enough to keep WebCCTV user logs for approximately 60 days.

5.2.4.1 Log Search

The search option allows you to retrieve all or specific actions that a certain user has performed.

Log Search Screen

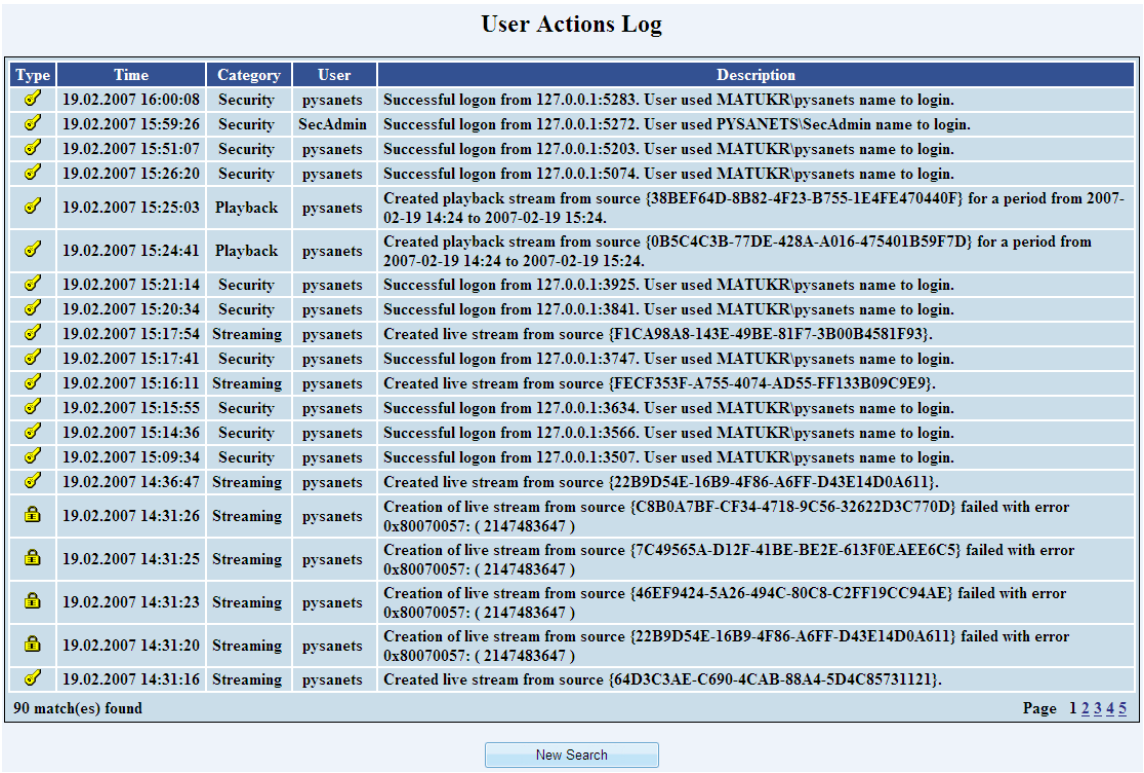
All possible actions are described in the following table and can be found in the picture above.

Category	Description
Security	Activity of the user's actions related to users management.
Streaming	Activity of the cameras that have been watched in live view.
Recording View	Activity of viewing video footage.
Export	Activity of video footage files that were made for exporting.

To do a search, follow the steps below:

1. Specify the user for which you want to search (Optional).
2. Define the time frame in which you want to search.
3. Check the required categories checkboxes.
4. Click the **Search** button.

The figure below provides a sample overview of a User Actions Log.



User Actions Log

Type	Time	Category	User	Description
	19.02.2007 16:00:08	Security	pysanets	Successful logon from 127.0.0.1:5283. User used MATUKR\pysanets name to login.
	19.02.2007 15:59:26	Security	SecAdmin	Successful logon from 127.0.0.1:5272. User used PYSANETS\SecAdmin name to login.
	19.02.2007 15:51:07	Security	pysanets	Successful logon from 127.0.0.1:5203. User used MATUKR\pysanets name to login.
	19.02.2007 15:26:20	Security	pysanets	Successful logon from 127.0.0.1:5074. User used MATUKR\pysanets name to login.
	19.02.2007 15:25:03	Playback	pysanets	Created playback stream from source {38BEF64D-8B82-4F23-B755-1E4FE470440F} for a period from 2007-02-19 14:24 to 2007-02-19 15:24.
	19.02.2007 15:24:41	Playback	pysanets	Created playback stream from source {0B5C4C3B-77DE-428A-A016-475401B59F7D} for a period from 2007-02-19 14:24 to 2007-02-19 15:24.
	19.02.2007 15:21:14	Security	pysanets	Successful logon from 127.0.0.1:3925. User used MATUKR\pysanets name to login.
	19.02.2007 15:20:34	Security	pysanets	Successful logon from 127.0.0.1:3841. User used MATUKR\pysanets name to login.
	19.02.2007 15:17:54	Streaming	pysanets	Created live stream from source {F1CA98A8-143E-49BE-81F7-3B00B4581F93}.
	19.02.2007 15:17:41	Security	pysanets	Successful logon from 127.0.0.1:3747. User used MATUKR\pysanets name to login.
	19.02.2007 15:16:11	Streaming	pysanets	Created live stream from source {FECF353F-A755-4074-AD55-FF133B09C9E9}.
	19.02.2007 15:15:55	Security	pysanets	Successful logon from 127.0.0.1:3634. User used MATUKR\pysanets name to login.
	19.02.2007 15:14:36	Security	pysanets	Successful logon from 127.0.0.1:3566. User used MATUKR\pysanets name to login.
	19.02.2007 15:09:34	Security	pysanets	Successful logon from 127.0.0.1:3507. User used MATUKR\pysanets name to login.
	19.02.2007 14:36:47	Streaming	pysanets	Created live stream from source {22B9D54E-16B9-4F86-A6FF-D43E14D0A611}.
	19.02.2007 14:31:26	Streaming	pysanets	Creation of live stream from source {C8B0A7BF-CF34-4718-9C56-32622D3C770D} failed with error 0x80070057: (2147483647)
	19.02.2007 14:31:25	Streaming	pysanets	Creation of live stream from source {7C49565A-D12F-41BE-BE2E-613F0EAEE6C5} failed with error 0x80070057: (2147483647)
	19.02.2007 14:31:23	Streaming	pysanets	Creation of live stream from source {46EF9424-5A26-494C-80C8-C2FF19CC94AE} failed with error 0x80070057: (2147483647)
	19.02.2007 14:31:20	Streaming	pysanets	Creation of live stream from source {22B9D54E-16B9-4F86-A6FF-D43E14D0A611} failed with error 0x80070057: (2147483647)
	19.02.2007 14:31:16	Streaming	pysanets	Created live stream from source {64D3C3AE-C690-4CAB-88A4-5D4C85731121}.

90 match(es) found Page 1 2 3 4 5

New Search

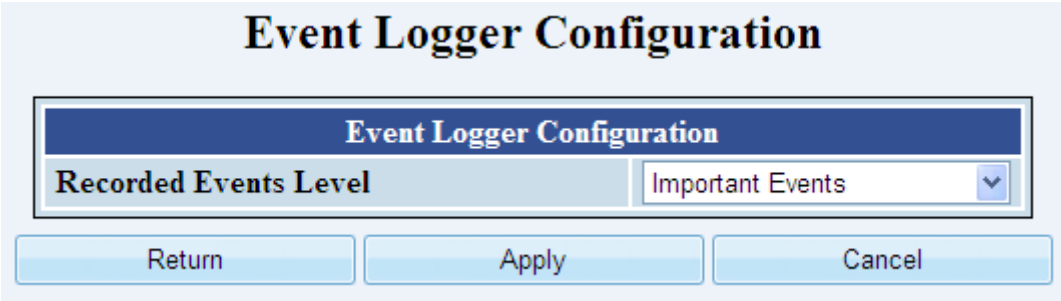
User Actions Logbook Screen

User Actions Log allows you to check all user actions at all times.

In order to conduct a new log search, click on the **New search** button. The reset filter button will clear all the checked boxes so that you can make a new selection.

5.2.4.2 Event Logger Configuration

The Event Logger Configuration defines the priority levels for the recorded events. Depending on the selected option, WebCCTV will or will not store certain events.



Event Logger Configuration Screen

There are three Recorded Events levels:

- **Only Critical Events** – WebCCTV stores the most important system events that occur when proper WebCCTV performance is impossible, e.g. recording break, failure to detect a system component, etc.

- **Important Events** – WebCCTV stores system events labelled as "Only Critical Events" and system events that play a significant role in the WebCCTV operating, e.g. playback stream creating, system logging on, etc.

- **All Events** – WebCCTV stores all system events.

To apply the new settings, click **Apply**.

To cancel your changes, click **Cancel.**

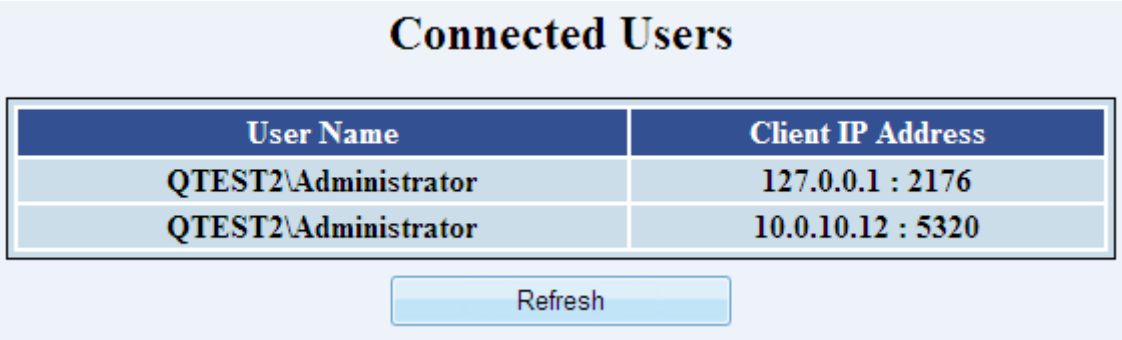
To go back to the Users Actions Log screen, click **Return**.

The Event Logger Settings functionality is unique for both User Actions Log and Server Actions Log.

5.2.5 Connected Users

This screen enables you to observe specific information about connected users such as:

- User Name
- Client IP-address



Connected Users Screen

In the Client IP address column you can observe two parameters, which are separated by a colon:

IP address is the IP address of the client computer from which a user is connected to the WebCCTV server.

Port number is the TCP port of the client computer from which a user is connected to the WebCCTV server.

Click the **Refresh** button to update the Connected Users list.

5.3 Settings

Settings Control Panel

The system Settings enable the user to change the WebCCTV behavior and adapt it to the specific requirements. This chapter covers the following sections:

- Cameras
- Alarms
- POS
- Storage Manager
- Single View
- Mosaics
- Network Settings
- Certificate Management

Use system Settings with extreme caution, some of them can seriously affect the WebCCTV performance and even stop proper functioning of the system.

Some of the system Settings require the WebCCTV to be rebooted for the settings to take effect. You will be informed to reboot the WebCCTV server by a red message on the screen. To restart the WebCCTV, click the **Restart** button which will turn red or click the **Restart now** link that appears at the end of the message. While restarting the server, you will get a message that the server is restarting. Once restarted, a successful reboot message will be displayed.

5.3.1 Cameras

The Cameras overview screen is automatically displayed, when entering the Settings menu.

WebCCTV supports both Analogue and Network cameras**.**

Analogue cameras can also be added and edited through a Network Video Server.

To **add a Network camera,** click the **Add IP Camera** and follow the on-screen instructions in the **Camera Wizard** (See **3.3.1.1 Camera Wizard**).

To **add a Network Video Server**, click the **Add Network Video Server** and follow the on-screen instructions in the **NVS Wizard** (See **3.3.1.2 Network Video Server Wizard**).

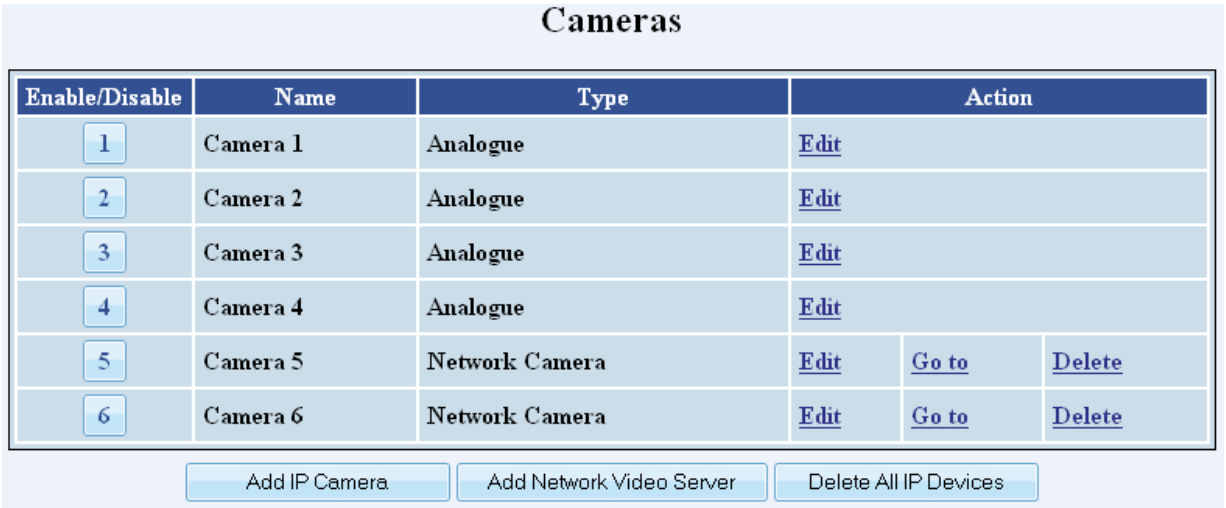
To **change Camera or Network Video Server settings,** click the **Edit** button to enter the **Camera** or **Network Video Server Wizard** which will guide you through the setting process for that camera or network video server.

To **directly access** a **Network camera** or a **Network Video Server,** click the **Go to** button. This function is available for IP-cameras only.

To **delete a Network camera,** click the **Delete** button.

To **delete a Network Video Server**, click the **Delete** button.

To **delete all IP devices,** click the **Delete All IP Devices** button.



Cameras Screen

To disable or enable a camera click its number. The button will become red when the camera is disabled in the system.

5.3.1.1 Camera Wizard

To enter the Camera Wizard click the **Edit** or the **Add IP Camera** button in the Cameras Screen. The Camera Wizard can consist of eight tabs with easy to follow instructions. Read this chapter to learn all about camera settings.

The following Camera Wizard tabs are described in this chapter:

- Name & Type
- Connection
- Live view
- Recordings
- Activity
- PTZ
- Virtual Patrol
- Users

By default, some of the settings are already selected. It is advisable to keep these settings to assure the best performance.

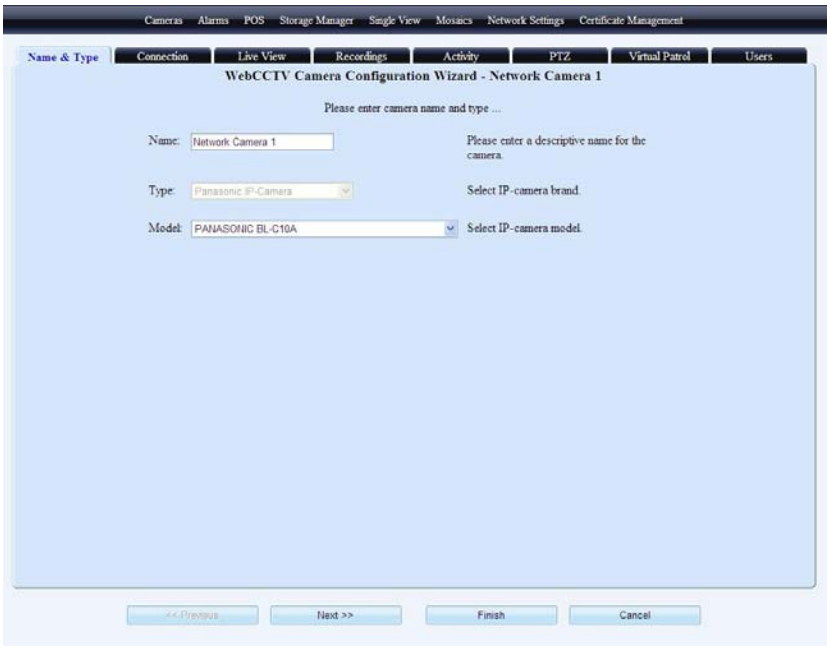
Depending on the camera type (network or analogue) and camera model, some tabs may not be present or may be disabled.

During the configuration, you may be asked to restart the server. This must be done first before finishing the configuration to assure the proper working of the WebCCTV server.

5.3.1.1.1 Name & Type

In this screen, you define the camera name, type and model of the camera.

Once the camera is added, you cannot change its type.



Name & Type (Network camera) Screen

Cameras Alarms POS Storage Manager Single View Mosaics Network Settings Certificate Management
Name & Type
Live View
Recordings
Activity
PTZ
Virtual Patrol
Users
WebCCTV Camera Configuration Wizard - Camera 1
Please enter camera name and type ...
Name: Camera 1
Please enter descriptive name for this camera.
Colour:
Please tick colour check-box if the connected camera is colour.
Video format: PAL NTSC
PAL colour video format is mostly used in Europe, NTSC video format is used in USA.
<< Previous
Next >>
Finish
Cancel

Name & Type (Analogue camera) Screen

Click **Next** to enter each camera and go to the next Camera Wizard screen.

5.3.1.1.2 Connection

This tab is only available for network cameras. If you are adding an analogue camera, this screen will not appear.

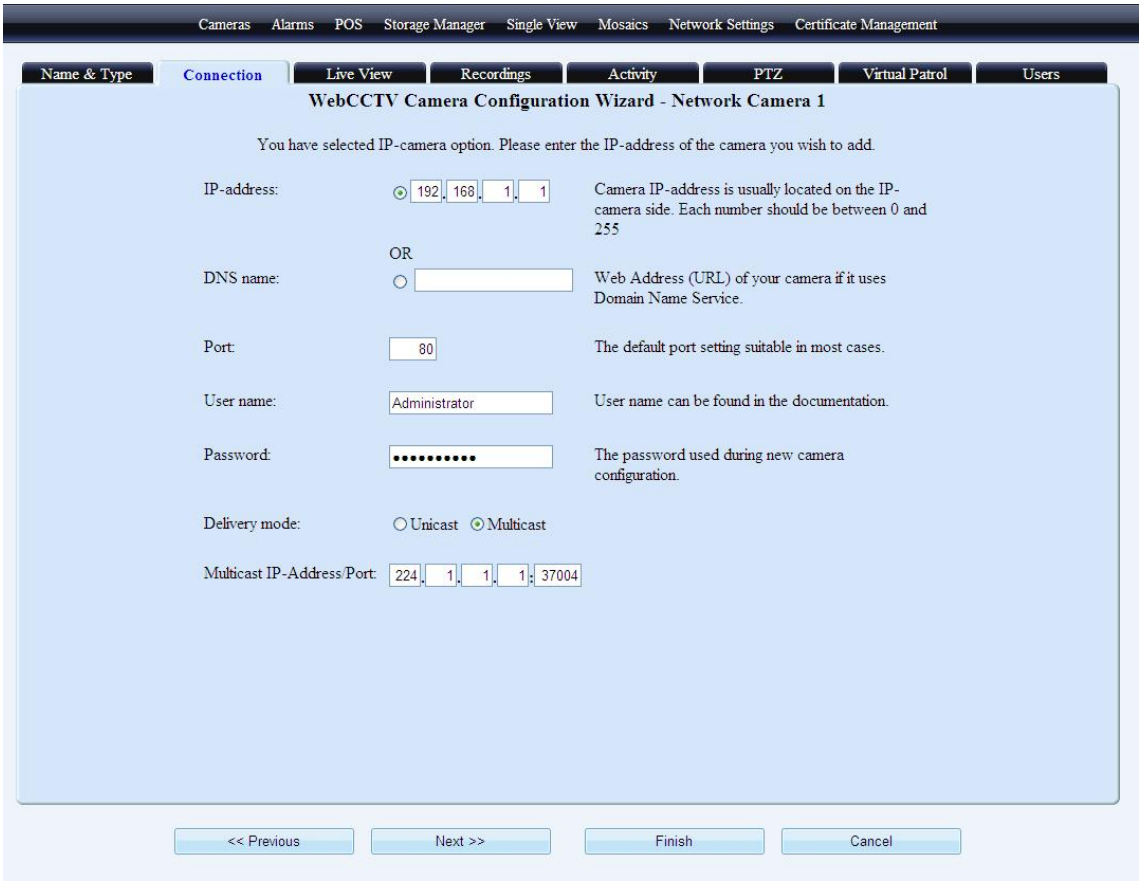
This screen allows you to define the parameters needed for a network camera connection:

- Camera IP address or DNS name
- Port
- User name
- Password
- Delivery mode
- Multicast IP-Address Port

To obtain these parameters, contact your system administrator or read the user manual of the camera itself.

Use camera **Administrator** credentials in order to get full WebCCTV functionality.

A DNS name is a meaningful and easy-to-remember "handle" for an Internet address or IP address.



Connection (Network camera) Screen

The delivery mode parameter is only available when the network camera supports MPEG streaming:

- **Unicast** – normal connection type of a camera. It is simple in organization and efficient when one connected client uses the camera. So if WebCCTV is the only user of the camera, please use this type.

- **Multicast** – this connection type is efficient when multiple applications use the cameras. This approach decreases the bandwidth usage. MPEG cameras allow sending the images to multicast IP addresses. These addresses are reserved in the IP protocol for multicast information distribution. To program a camera to send the images to a multicast address, you have to configure it in the camera's native software software. Specify the IP address on the Connection Screen of the camera wizard.

Multicast IP addresses are in the range 224.0.0.0 through 239.255.255.255.

Click **Next** to enter the next Camera Wizard screen.

5.3.1.1.3 Live View

The Live View tab will appear differently depending on whether you are viewing Analogue or IP cameras.

The following parameters can be set for an analogue camera:

- **Image resolution** – as a rule of thumb, the higher the quality of the image (higher image resolution), the lower the frame rate you will have.
- **Differential transmission** – when differential transmission is enabled, only the differences between subsequent images are sent over the network. This feature drastically decreases the amount of transmitted video-data and is especially designed to be used when viewing camera images over the Internet.

Cameras
Alarms
POS
Storage Manager
Single View
Mosaics
Network Settings
Certificate Management
Name & Type
Live View
Recordings
Activity
PTZ
Virtual Patrol
Users
WebCCTV Camera Configuration Wizard - Camera 1
Please choose live view resolution...
Remember that there is always a trade-off between image quality and frame rate - the bigger and better image you choose, the less frame rate WebCCTV can achieve
Image resolution:
384x288
768x288
768x576
Differential transmission:
Differential transmission drastically decreases the amount of data sent over the network. Please note that this transmission option will slightly increase CPU consumption at the WebCCTV Server side and slightly change live view quality.
<< Previous
Next >>
Finish
Cancel

Live View (Analogue camera) Screen

The following parameters can be set for a network camera:

- **Format** – gives an opportunity to choose between commonly used compression technologies or indicates the compression technology that is used for a specific camera type.

- **Image resolution** – a higher resolution gives a better quality image. A higher image resolution will lead to a lower frame rate.

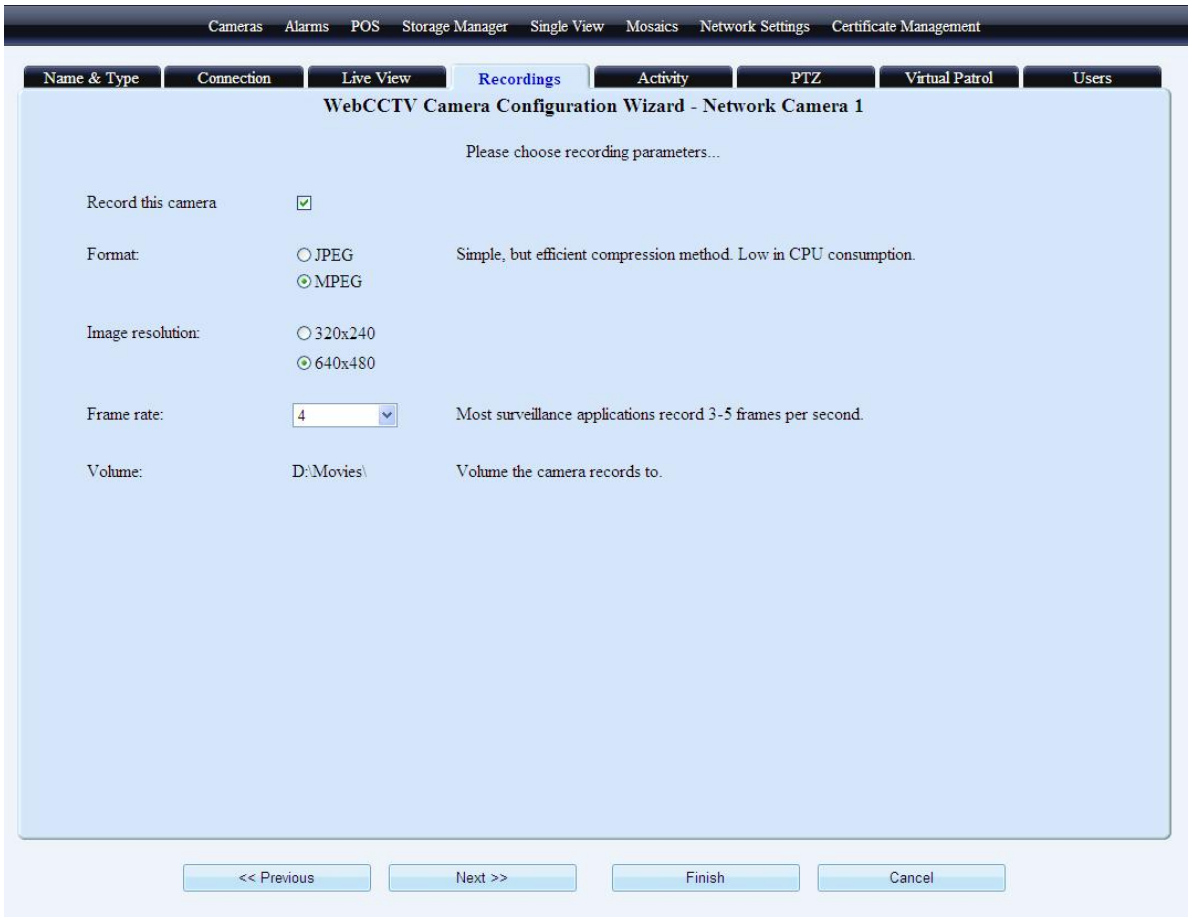
Live View (Network camera) Screen

Click **Next** to enter the next Camera Wizard screen.

5.3.1.1.4 Recordings

The available parameters for recordings are the same for analogue and network cameras:

- **Record this camera** – the camera will be recorded if the box is checked.
- **Format** – gives the option to choose between commonly used compression technologies or indicates the compression technology that is used for a specific camera type.
- **Image resolution** – a higher resolution gives a better quality image. A higher image resolution will lead to a lower frame rate.
- **Frame rate** – possible frame rates depend on the chosen image resolution.
- **Volume** – the storage volume on which the camera is recorded. You can change the volume for each camera (see ***3.3.4 Storage Manager***)



Recordings (analogue and network camera) Screen

Click **Next** to enter the next Camera Wizard screen.

5.3.1.1.5 Activity

In this screen, you can adjust the following parameters:

When adding a network camera, the Masking and Activity functionality is only available after a server restart. This will be requested automatically by a notification.

- **Activity Detection** – by enabling Activity Detection, only images where movement is above a certain threshold will be recorded. This increases the ability to store more video footage significantly. If you want to record all the time, uncheck the **Record only activity** checkbox.

The current activity level is represented by the green line on the control panel below the video. To adjust the activity detection threshold, move the slider on the right side of the control panel up and down to shift the red line. All the video activity that stays above the red line will be recorded.

- **Masking** – by using the masking feature, only activity in a specified area(s) will be recorded. This significantly increases the ability to store video footage.

Cameras
Alarms
POS
Storage Manager
Single View
Mosaics
Network Settings
Certificate Management
Name & Type
Connection
Live View
Recordings
Activity
PTZ
Virtual Patrol
Users
WebCCTV Camera Configuration Wizard - Network Camera 1
Please select the desired activity detection level...
Mask
Unmask
Apply Mask
?
Record only activity
Recording only meaningful activity allows you to record for a longer period and makes searching in the video more efficient.
Activity detection can be visually adjusted to the desired level, provided a camera is connected. Current video activity level is represented by the green line on the control panel below the video.
To adjust video activity, move the slider on the right side of the control panel up and down to shift the red line. All the video activity that stays above the red line will be recorded.
100
0
<< Previous
Next >>
Finish
Cancel

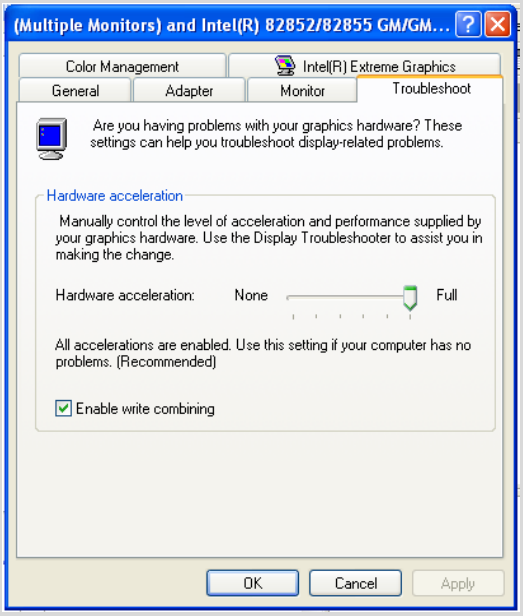
Activity (analogue and network camera) Screen

Masking makes it possible to disable the recording of activity in so called 'curtain areas'. 'Curtain areas' contain constant movement classified as not important for surveillance (e.g. moving trees in the wind, ceiling fan etc.).

The green grid, shown on the masking screen, divides the image into masking cells. Click on a cell and the activity detection in this cell will be disabled. Once disabled, a masking cell turns green. This means that activity occurring in this cell will not trigger recording.

When you access the Activity screen for the first time on a client PC, it may be that the green masking grid doesn't appear. In order to be able to draw the grid, the video card of the client PC has to have at least 16 MB of internal video memory and DirectX accelerations fully enabled. This can be done as follows:

1. Exit the camera wizard by clicking **Finish** or **Cancel**.
2. Go to Start/Settings/**Control Panel**.
3. Click on Display/ Settings/Advanced/**Troubleshoot**.
4. Set **Hardware acceleration** on full.


(Multiple Monitors) and Intel(R) 82852/82855 GM/GM...
Color Management
Intel(R) Extreme Graphics
General
Adapter
Monitor
Troubleshoot
Are you having problems with your graphics hardware? These settings can help you troubleshoot display-related problems.
Hardware acceleration
Manually control the level of acceleration and performance supplied by your graphics hardware. Use the Display Troubleshooter to assist you in making the change.
Hardware acceleration:
None
Full
All accelerations are enabled. Use this setting if your computer has no problems. (Recommended)
Enable write combining
OK
Cancel
Apply

Troubleshoot Screen

Click **OK** and return to the Activity Screen in the Camera Wizard. The masking grid should be visible on your screen now.

The masking functionality does not depend on whether you can visualize it on a particular client PC or not. It is possible to set up masking on one client PC and use another client PC which is not able to show masking. The masking will stay applied.

To (un)mask the desired area, follow the steps below:

1. Click on the cell you wish to (un)mask.
2. Check the **Mask** or **Unmask** button depending on whether you want to mask or unmask.
3. Click the **Apply mask** button to activate the selection.

To mask multiple cells, left-click one cell and drag the cursor over the cells you would like to mask and release your mouse.

Click on the question mark icon in the right hand corner of the masking screen to access on-screen masking instructions.

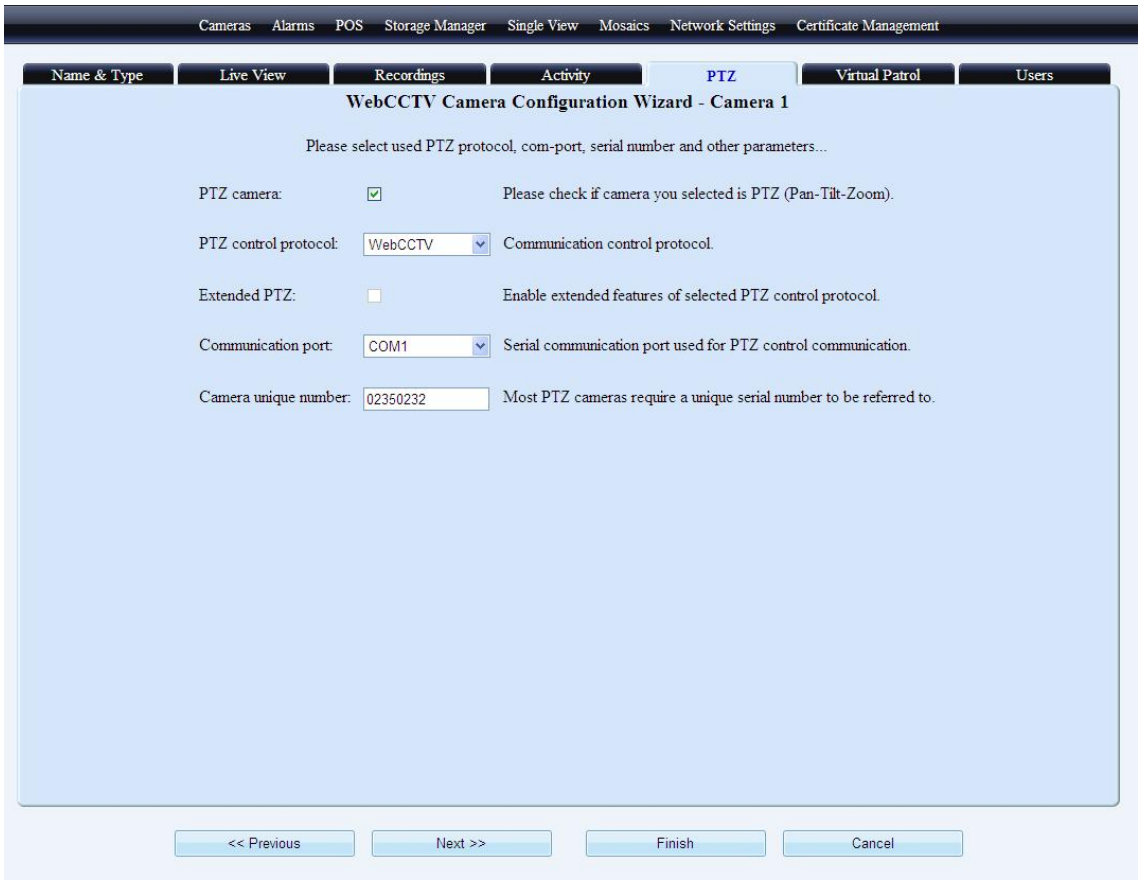
Click **Next** to enter the next Camera Wizard screen.

5.3.1.1.6 PTZ

This tab is present for both analogue and network PTZ cameras, however only **analogue PTZ cameras** can be configured

PTZ stands for Pan Tilt Zoom, or a "movable" camera. To enable the PTZ camera settings, select the PTZ camera check box .

- **PTZ camera** – check this if your camera is a PTZ camera
- **PTZ control protocol** – select the brand of the PTZ camera
- **Extended PTZ** – Some protocols have extended PTZ features; e.g. Pelco. By checking this, these extended features will be made available.
- **Communication port** – serial communication port used for PTZ communication.
- **Camera unique number** – most PTZ cameras require a unique serial number to be referred by.



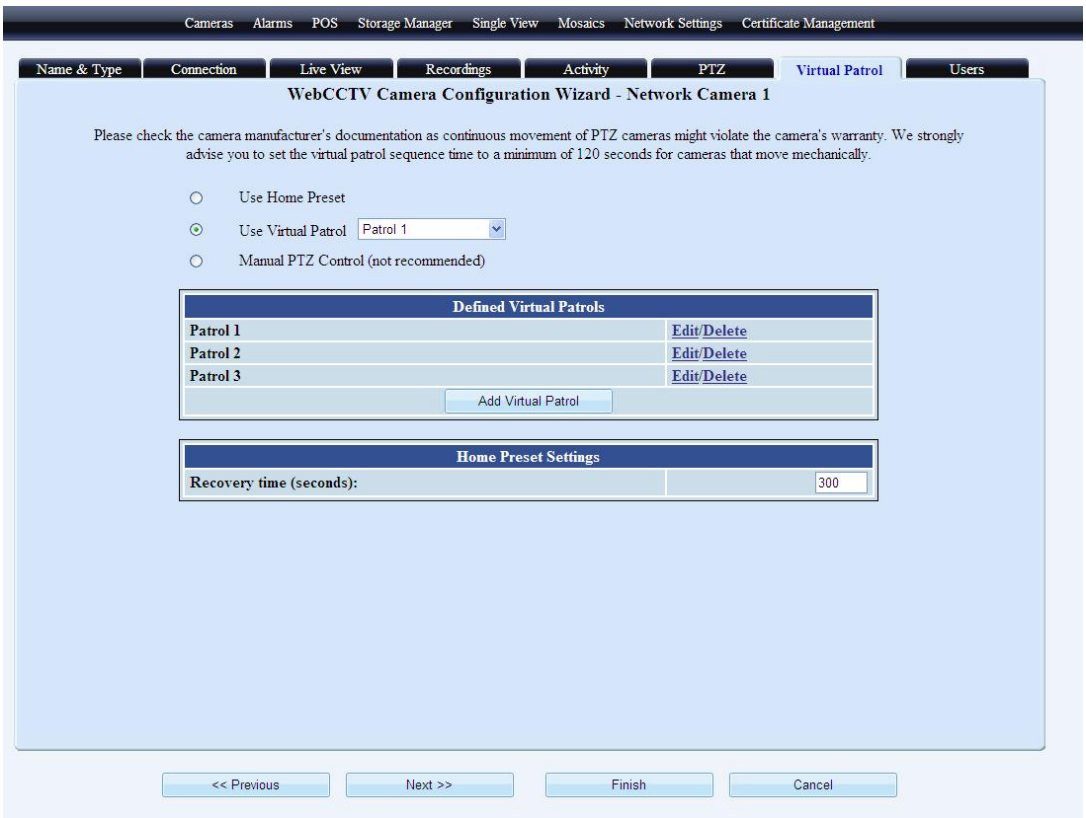
PTZ (analogue PTZ camera) Screen

Click **Next** to enter the next Camera Wizard screen.

5.3.1.1.7 Virtual Patrol

The Virtual Patrol screen allows you to configure a PTZ camera in several ways:

- **Use Home preset** – this functionality prevents the misplacement of the camera and ensures proper recordings after monitoring. If the **Home Preset** is enabled, the first preset position becomes automatically the **Home** status and looks like in the **Live view**. When a user moves the PTZ camera, by manual manipulation or using preset positions, the camera will return to its Home Preset after the assigned **Recovery Time** has elapsed. By default this time is 300 seconds.
- **Use Virtual Patrol** – select one of the Virtual Patrols you previously created.
- **Manual PTZ Control** – check this radio button if you don't use either the Home Preset or the Virtual Patrol functionality.



Virtual Patrol (analogue and network camera) Screen

Only specially designed cameras designated by the manufacturer as "Continuous movement use", "Continuous duty cycle" or "24h duty cycle" can effectively utilize the Virtual Patrol feature. Using consumer-grade cameras with Virtual Patrol may cause premature failure and may invalidate the cameras warranty. We strongly advise customers to check the camera specifications before using the Virtual Patrol feature and strongly advise setting the virtual patrol sequence time to a minimum of 120 seconds for those cameras.

You can create multiple Virtual Patrols with different settings. Click the **Add Virtual Patrol** button to add a new Virtual Patrol.

To change or create the Virtual Patrol settings, click the **Edit** link.

Virtual Patrol Configuring Screen

1. Specify a **Name** for the Virtual Patrol
2. Choose one of the available Presets from the drop-down list and click **Add Preset** button.
3. Specify the **Sequence time** for every Preset. This is the time after which the camera is switched to the next defined preset in the queue.
4. If necessary, use the **Sort** buttons to change the position of a Preset in the Virtual Patrol sequence.
5. Click **Apply** button.

You may delete any Preset from the Virtual Patrol sequence by clicking the **Delete** link.

Due to some technology designs of Panasonic cameras, it is recommended to use no more than 2-3 Panasonic cameras with virtual patrol configured at the same time, since this can cause server overloading.

Each time a user takes control over the PTZ camera manually (via the PTZ Camera Control Panel), the automatic Virtual Patrol is interrupted. Once the user stops his manual control, the WebCCTV resumes the Virtual Patrol after 30 seconds.

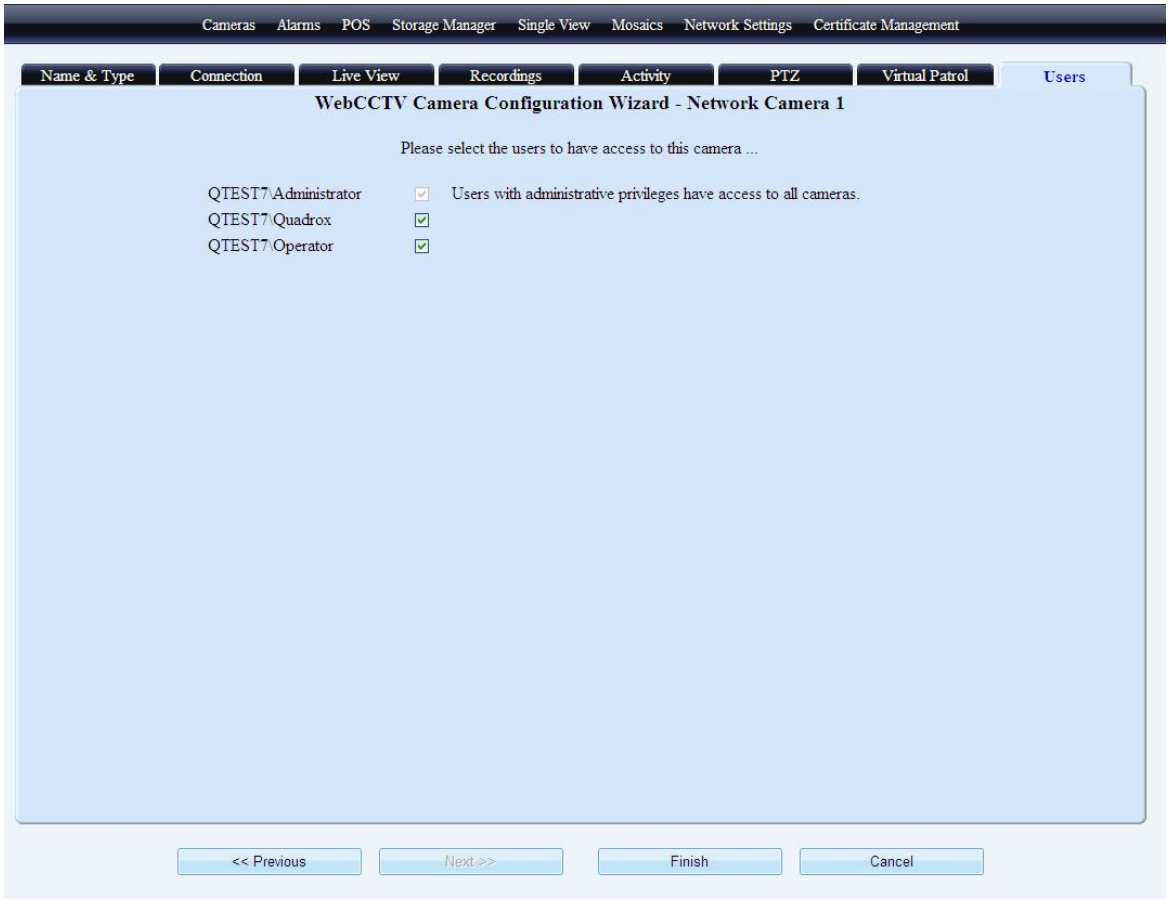
Click **Next** to enter the next Camera Wizard screen.

5.3.1.1.8 Users

Select which users have access to the selected camera.

The Users functionality is only available after you have added the camera, and restarted the server. Follow the notification that will automatically be shown.

Users with Administrator rights have access to all cameras. Users with restricted rights can be denied access to certain cameras.



Users (analogue and network camera) Screen

5.3.1.2 Network Video Server Wizard

In this manual, we will refer to a **Network Video Server** as **NVS**.

To enter the Network Video Server Wizard, click the **Edit Device** or **Add Network Video Server** link/button in the Cameras screen. The **Network Video Server Wizard** consists of three tabs with easy to follow instructions.

The following **Network Video Server Wizard** tabs are described in this chapter:

- Name & Type
- Connection
- Video Settings

If you need to change camera settings from cameras that are connected to the NVS, click the **Edit** link of the camera in the cameras screen which will display the Network Video Server Cameras Wizard. The **Network Video Server Camera Wizard** consists of six tabs with easy to follow instructions.

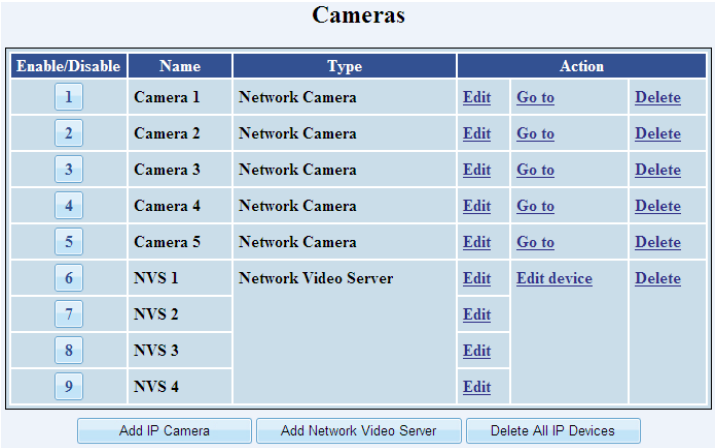
The following **Network Video Server Camera Wizard** tabs are described in this chapter:

- Name
- Recordings
- Activity
- PTZ
- Virtual Patrol
- Users

You need to install the **Quadrox Codecs Pack** for proper NVS usage. (http://www.webcctv.com/ftp/Documentation/Quadrox_Codec_Pack_Installation_Manual.pdf)

The NVS Wizard displays settings which are common for all cameras connected to the NVS. In the NVS Camera Wizard you are able to adjust the specific settings for an individual camera connected to the NVS.

By default, some of the settings are already selected. It is recommended that you keep these settings to ensure the best performance.

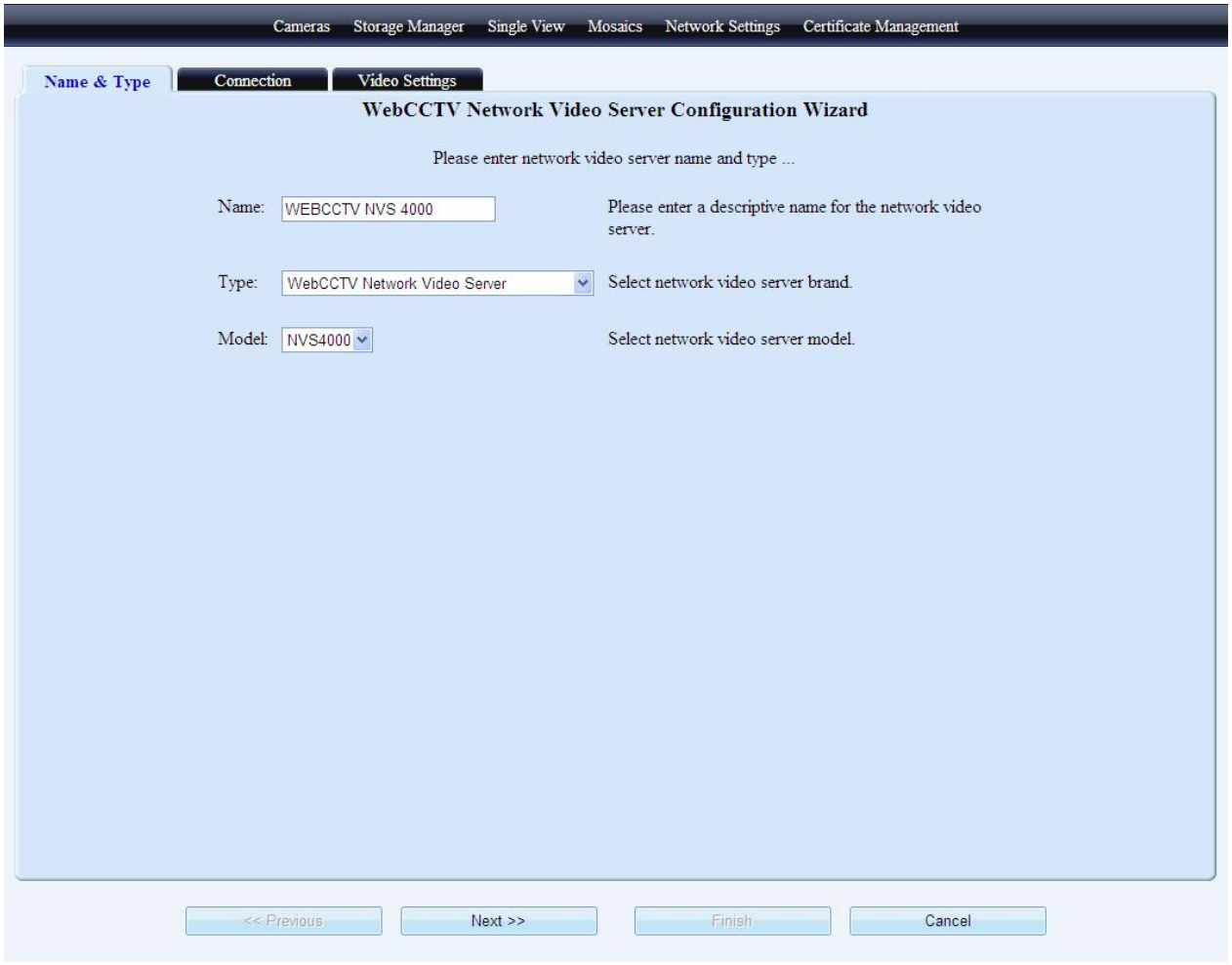

Cameras
Enable/Disable
Name
Type
Action
1 Camera 1 Network Camera Edit Go to Delete
2 Camera 2 Network Camera Edit Go to Delete
3 Camera 3 Network Camera Edit Go to Delete
4 Camera 4 Network Camera Edit Go to Delete
5 Camera 5 Network Camera Edit Go to Delete
6 NVS 1 Network Video Server Edit Edit device Delete
7 NVS 2 Edit
8 NVS 3 Edit
9 NVS 4 Edit
Add IP Camera
Add Network Video Server
Delete All IP Devices

Cameras Screen

5.3.1.2.1 Name & Type

In this tab, you can adjust the NVS name, type and model. It's a part of the **Network Video Server Wizard.**

Choose a descriptive name for each NVS for easy future reference.



Name & Type (Network Video Server) Screen

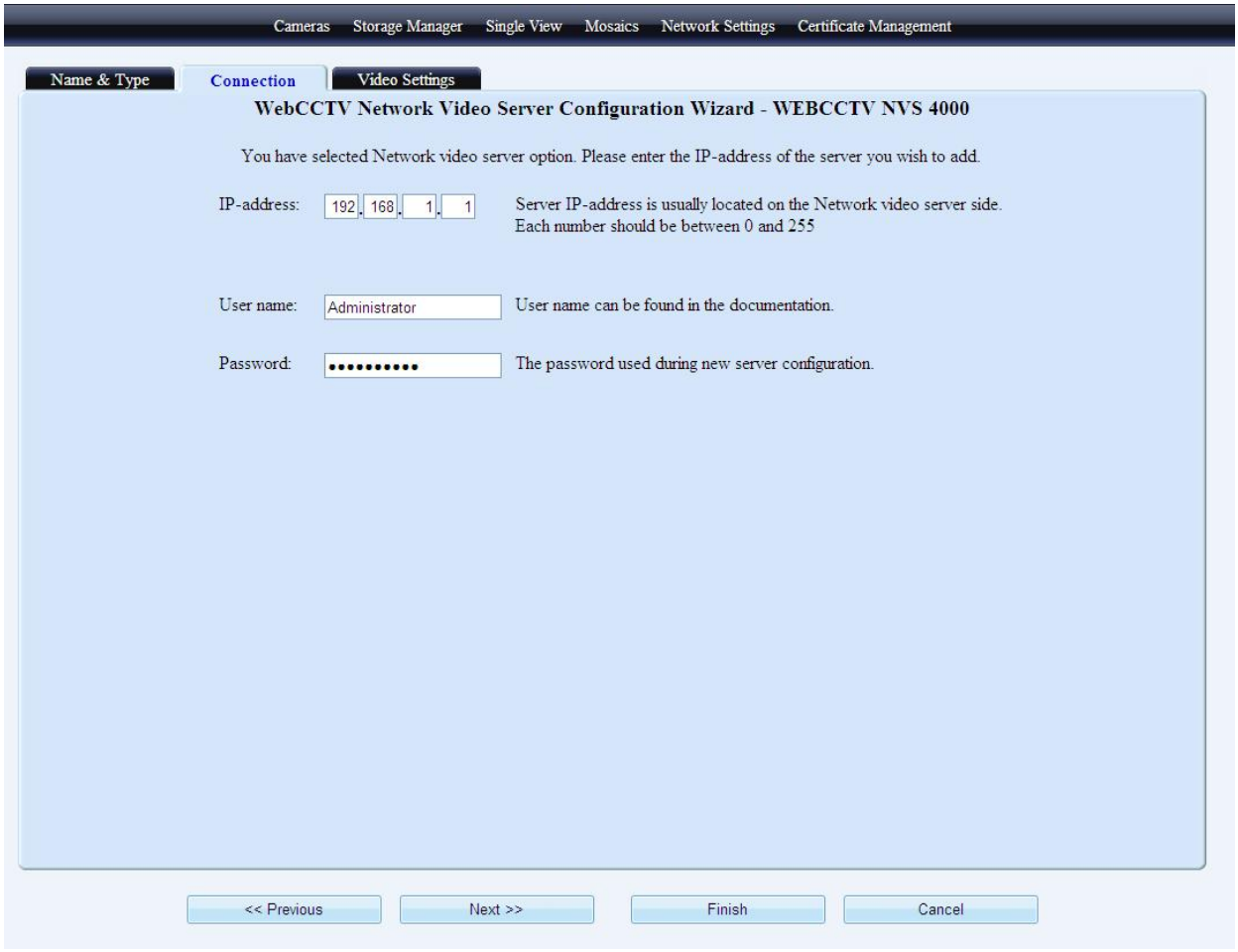
Click **Next** to enter the next NVS Wizard screen.

5.3.1.2.2 Connection

This tab allows you to define the parameters needed for the NVS connection. It's a part of the **Network Video Server Wizard**:

- NVS IP address
- User name
- Password

The Default Admin ID for the NVS400 series is 'admin' and the default Admin password is 'pass'. For the NVS1000/2000/4000 series the Admin ID becomes 'root' and the default Admin password is 'pass'.


Cameras
Storage Manager
Single View
Mosaics
Network Settings
Certificate Management
Name & Type
Connection
Video Settings
WebCCTV Network Video Server Configuration Wizard - WEBCCTV NVS 4000
You have selected Network video server option. Please enter the IP-address of the server you wish to add.
IP-address:
192 . 168 . 1 . 1
Server IP-address is usually located on the Network video server side.
Each number should be between 0 and 255
User name:
Administrator
User name can be found in the documentation.
Password:
The password used during new server configuration.
<< Previous
Next >>
Finish
Cancel

Connection (Network Video Server) Screen

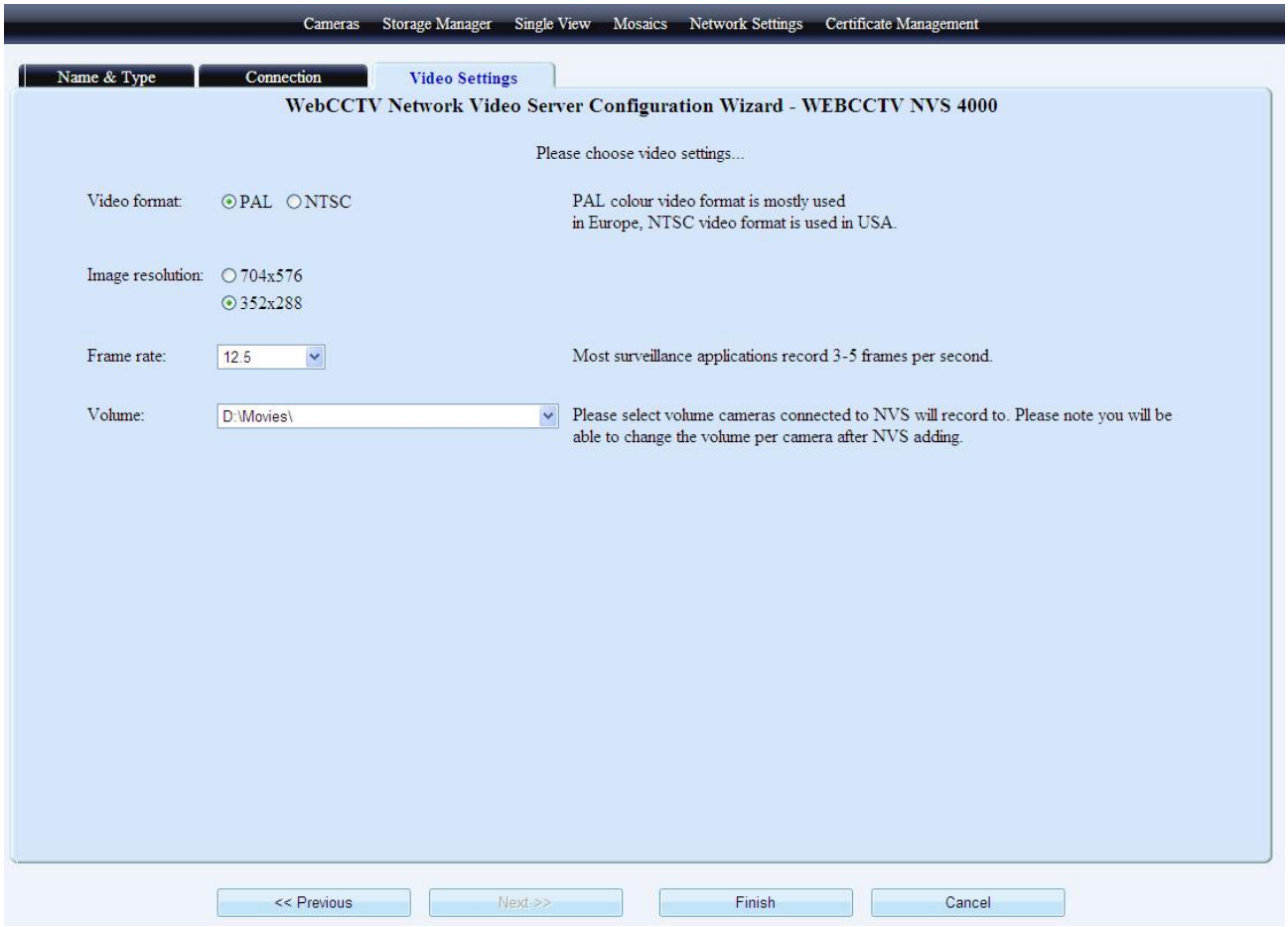
Click **Next** to enter the next NVS Wizard screen.

5.3.1.2.3 Video Settings

This tab is a part of the **Network Video Server Wizard** and allows configuring following settings:

- **Video format** – selection of the video standards format in which images are transmitted from the cameras. PAL video standard is used in Europe, NTSC video standard is used in the USA.
- **Image resolution** – a higher resolution gives a better quality image. A higher image resolution will lead to a lower frame rate.
- **Frame rate** – possible frame rates depend on the chosen image resolution.
- **Volume** – storage volume on which the camera is recorded. You can change the volume for each camera (see ***3.3.4 Storage Manager***)

Settings you are adjusting in this screen are applied to all NVS cameras for live view and recordings.

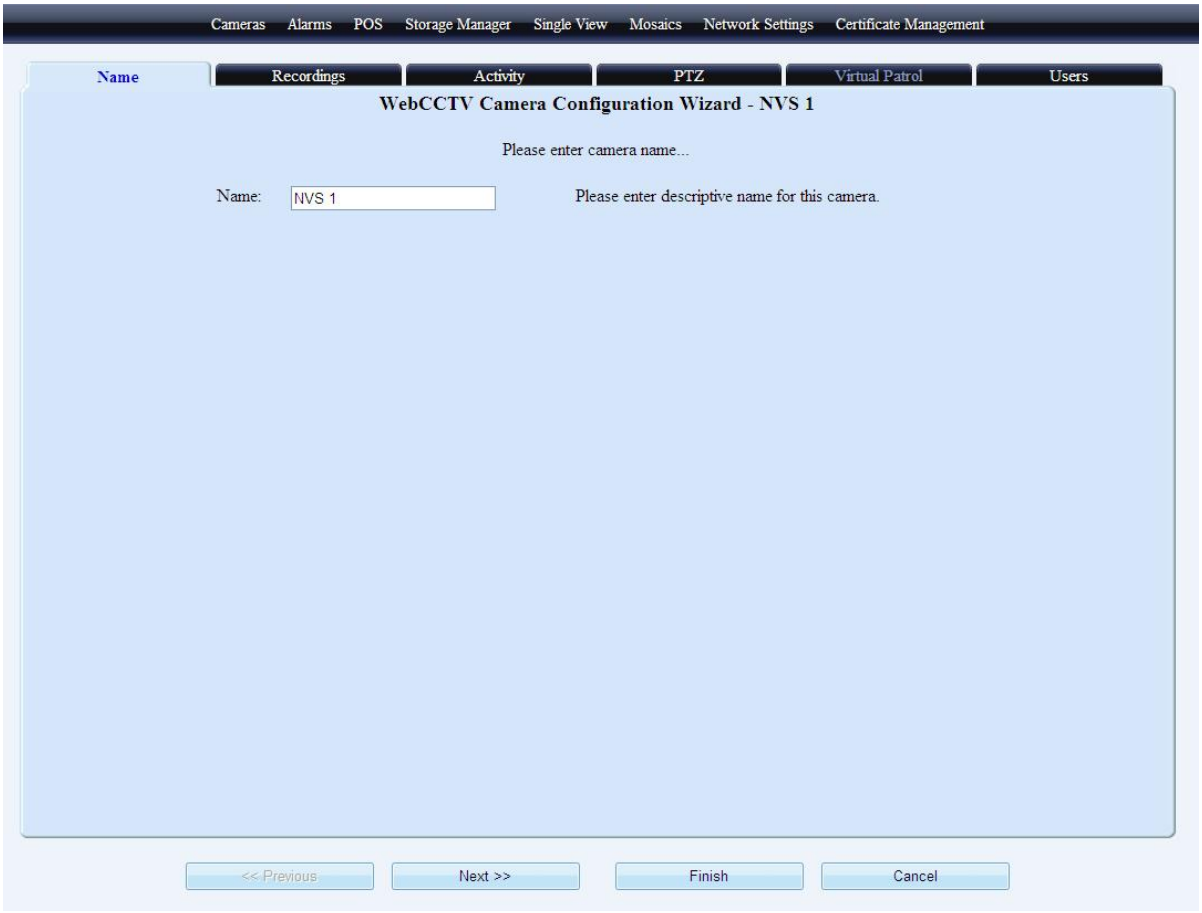


Video Settings (Network Video Server) Screen

Complete the procedure by clicking **Finish** button and **Restart** the WebCCTV server.

5.3.1.2.4 Name

This tab is a part of the **Network Video Server Camera Wizard**. You can assign a **name** to the camera in this screen.



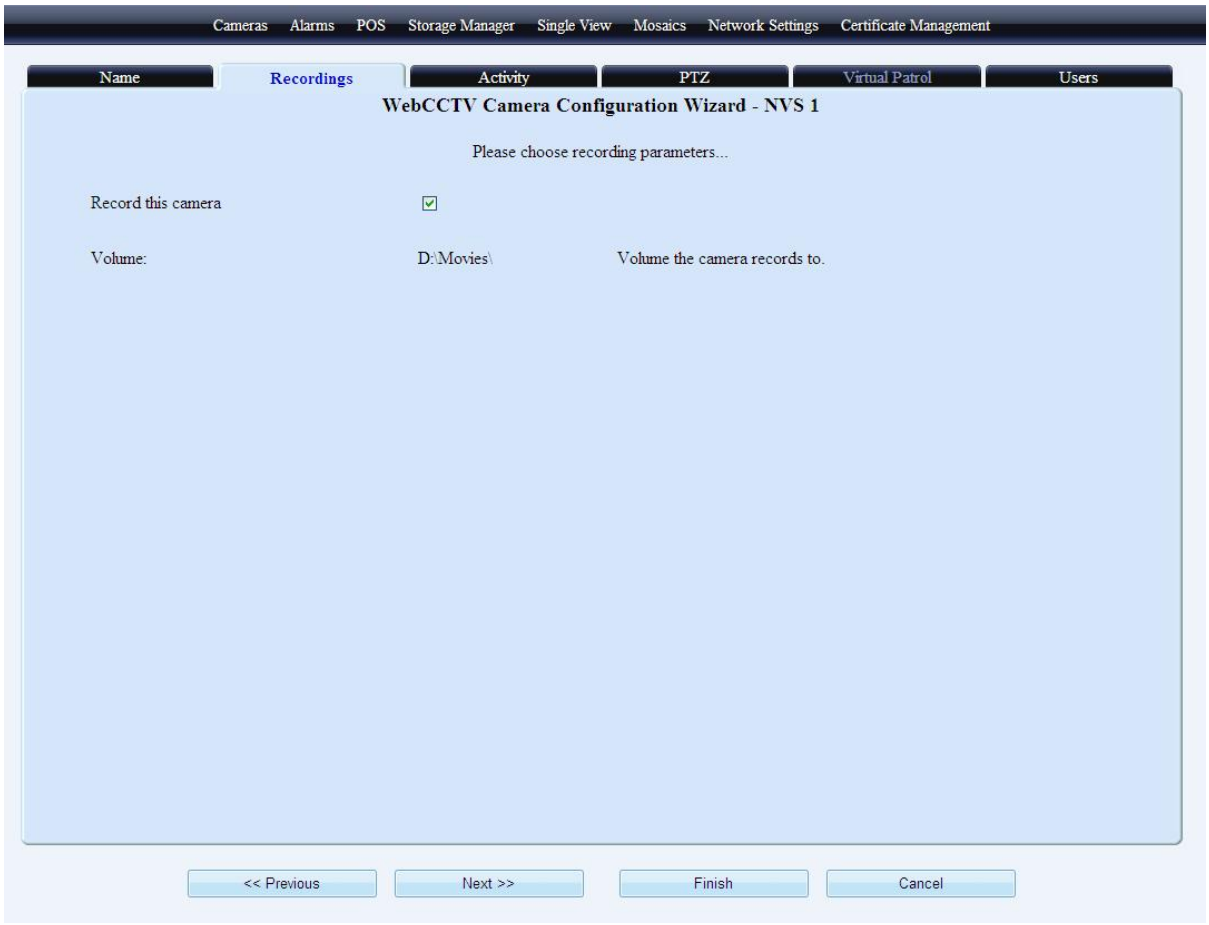
Name (Network Video Server) Screen

Click **Next** to enter the next NVS Camera Wizard screen.

5.3.1.2.5 Recordings

This tab is a part of the **Network Video Server Camera Wizard**. The following parameters can be configured:

- **Record this camera** – the camera will be recorded if the box is checked.
- **Volume** – storage volume on which the camera is recorded. You can change the volume for each camera (see ***3.3.4 Storage Manager***)



Recordings (Network Video Server) Screen

Click **Next** to enter the next NVS Camera Wizard screen.

5.3.1.2.6 Activity

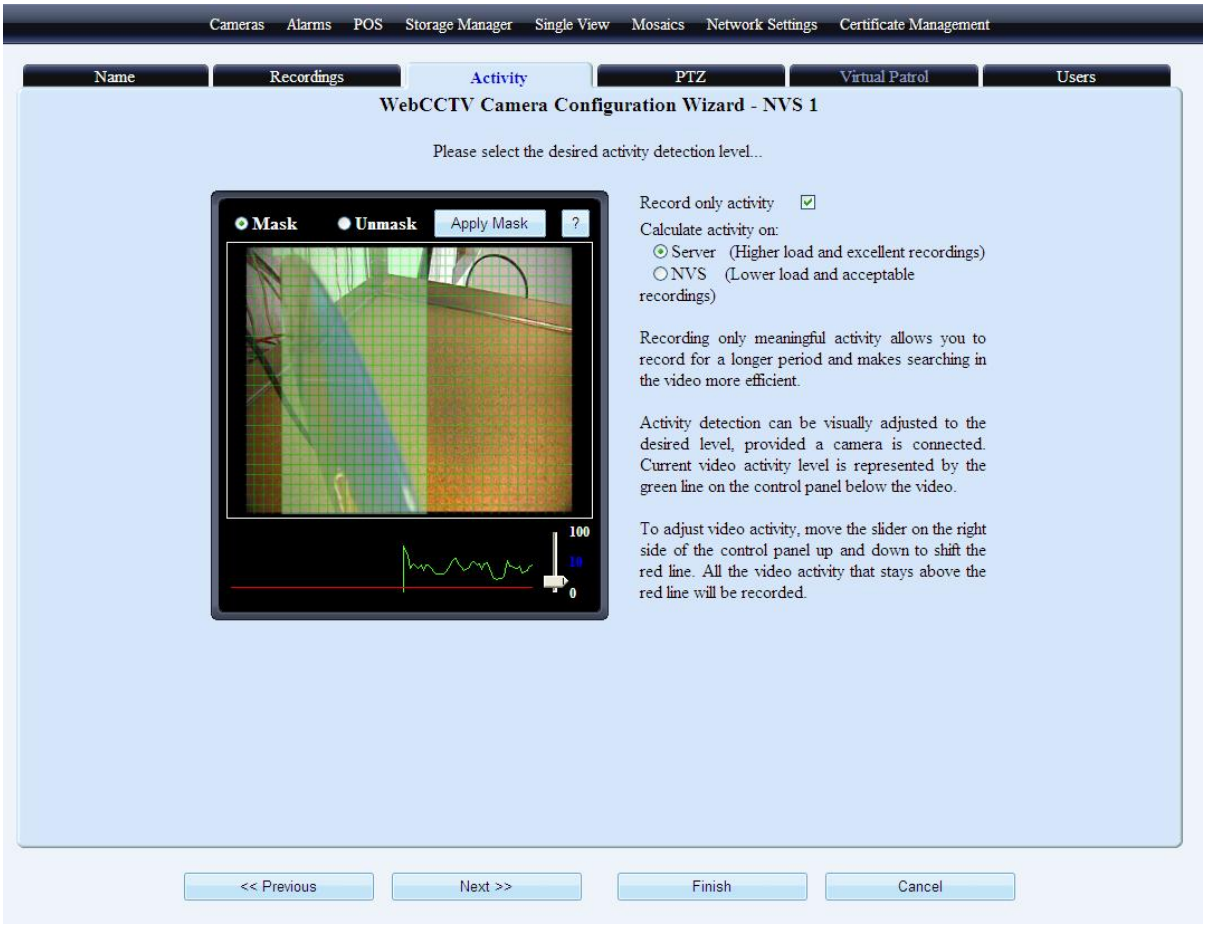
This tab is a part of the **Network Video Server Camera Wizard**. The following parameters can be configured:

When adding a NVS, the Masking and Activity functionality is only available after server restart. This will be automatically requested by a notification.

- **Activity Detection** – by enabling Activity Detection, only images where movement is above a certain threshold will be recorded. This increases the ability to store more video footage significantly. If you want to record all the time, uncheck the **Record only activity** checkbox.

The current activity level is represented by the green line on the control panel below the video. To adjust the activity detection threshold, move the slider on the right side of the control panel up and down to shift the red line. All the video activity that stays above the red line will be recorded.

- **Masking** – by using the masking feature, only activity in a specified area(s) will be recorded. This increases the ability to store more video footage significantly.


Cameras
Alarms
POS
Storage Manager
Single View
Mosaics
Network Settings
Certificate Management
Name
Recordings
Activity
PTZ
Virtual Patrol
Users
WebCCTV Camera Configuration Wizard - NVS 1
Please select the desired activity detection level...
Mask
Unmask
Apply Mask
?
100
10
0
Record only activity
Calculate activity on:
Server (Higher load and excellent recordings)
NVS (Lower load and acceptable recordings)
Recording only meaningful activity allows you to record for a longer period and makes searching in the video more efficient.
Activity detection can be visually adjusted to the desired level, provided a camera is connected. Current video activity level is represented by the green line on the control panel below the video.
To adjust video activity, move the slider on the right side of the control panel up and down to shift the red line. All the video activity that stays above the red line will be recorded.
<< Previous
Next >>
Finish
Cancel

Activity (Network Video Server) Screen

- **Calculate activity on** – Each method of activity detection processing has advantages and disadvantages. Activity detection processing on the WebCCTV server allows

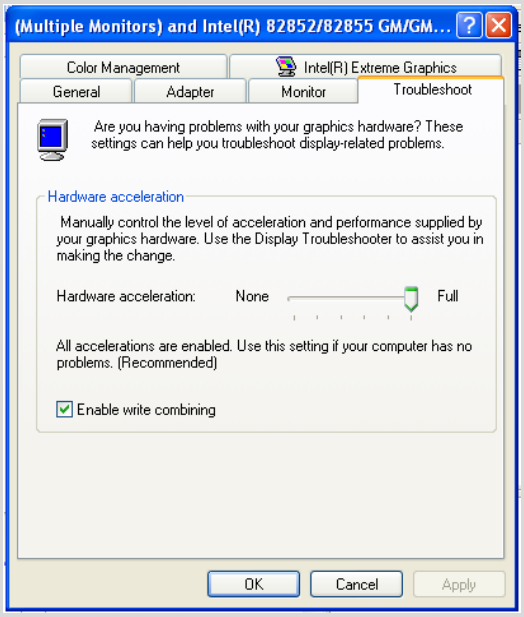
detecting the activity using the best accuracy, but consumes more CPU resources. Activity detection processing on WebCCTV NVS consumes fewer CPU resources, but operates inaccurately in low light conditions.

Masking makes it possible to disable the recording of activity in so called 'curtain areas'. 'Curtain areas' contain constant movement classified as not important for surveillance (e.g. moving trees in the wind, busy parts of the road etc.).

The green grid, shown on the masking screen, divides the image into masking cells. Click on a cell and the activity detection in this cell will be disabled. Once disabled, a masking cell turns green. This means that activity occurring in this cell will not trigger recording.

When you access the Activity screen for the first time on a client PC, it may be that the green masking grid doesn't appear. In order to be able to draw the grid, the video card of the client PC has to have at least 16 MB of internal video memory and DirectX accelerations fully enabled. This can be done as follows:

1. Exit the camera wizard by clicking **Finish** or **Cancel**.
2. Go to Start/Settings/**Control Panel**.
3. Click on Display/ Settings/Advanced/**Troubleshoot**.
4. Set **Hardware acceleration** on full.


(Multiple Monitors) and Intel(R) 82852/82855 GM/GM...
Color Management
Intel(R) Extreme Graphics
General
Adapter
Monitor
Troubleshoot
Are you having problems with your graphics hardware? These settings can help you troubleshoot display-related problems.
Hardware acceleration
Manually control the level of acceleration and performance supplied by your graphics hardware. Use the Display Troubleshooter to assist you in making the change.
Hardware acceleration:
None
Full
All accelerations are enabled. Use this setting if your computer has no problems. (Recommended)
Enable write combining
OK
Cancel
Apply

Troubleshoot Screen

Click **OK** and return to the Activity Screen in the Camera Wizard. The masking grid should be visible on your screen now.

The masking functionality does not depend on whether you can visualize it on a particular client PC or not. It is possible to set up masking on one client PC and use another client PC which is not able to show masking. The masking will stay applied.

To (un)mask the desired area, follow the steps below:

1. Click on the cell you wish to (un)mask.
2. Check the **Mask** or **Unmask** button depending on whether you want to mask or unmask.
3. Click the **Apply mask** button to activate the selection.

To mask multiple cells, left-click one cell and drag the cursor over the cells you would like to mask and release your mouse.

Click on the question mark icon in the right hand corner of the masking screen to access on-screen masking instructions.

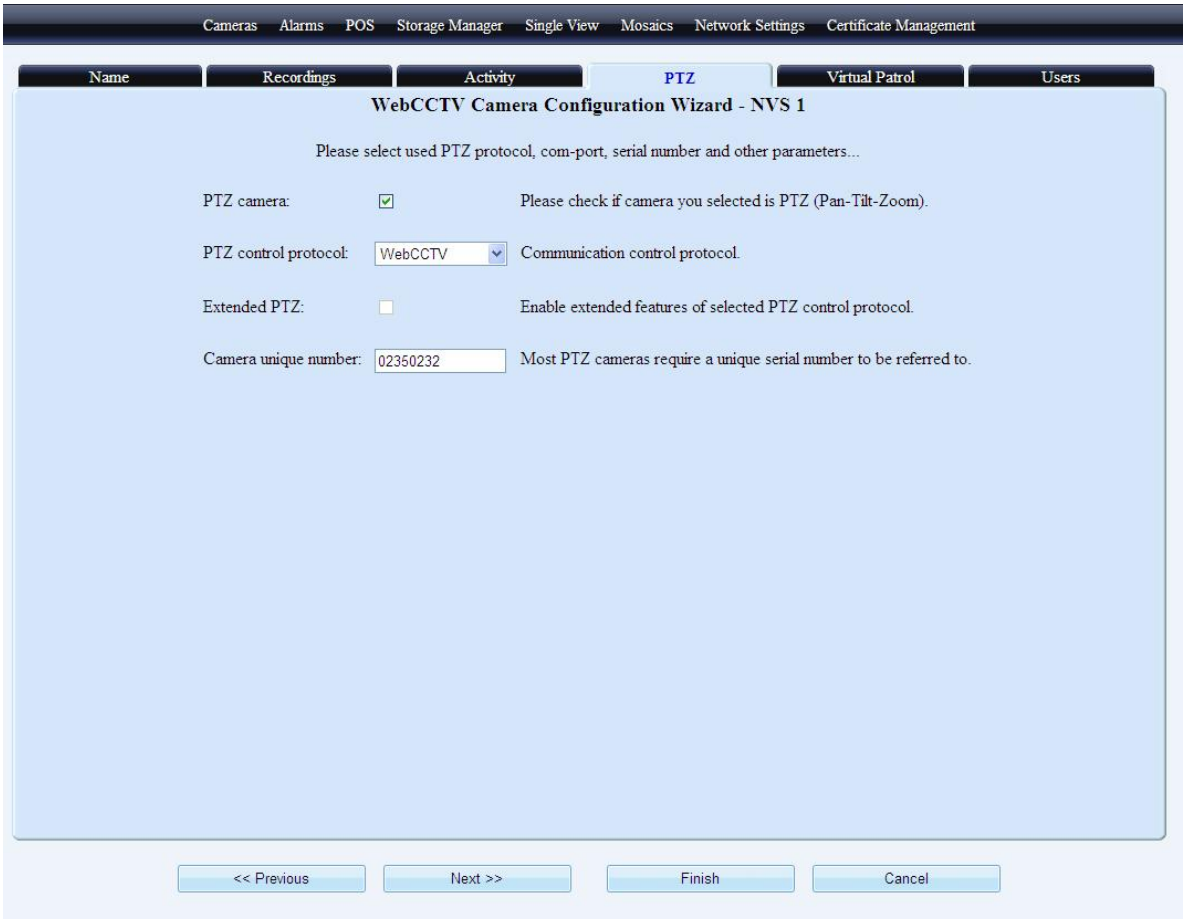
Click **Next** to enter the next NVS Camera Wizard screen.

5.3.1.2.7 PTZ

This tab is a part of the **Network Video Server Camera Wizard**.

PTZ stands for Pan Tilt Zoom or movable camera. To enable PTZ camera settings, select the PTZ camera check box first.

- **PTZ camera** – select this if your camera is a PTZ camera.
- **PTZ control protocol** – select the brand of the PTZ camera.
- **Extended PTZ** – Some protocols have extended PTZ features, e.g. Pelco. By checking this, the features will be made available.
- **Camera unique number** – most PTZ cameras require a unique serial number to be referred by.



PTZ (Network Video Server) Screen

Click **Next** to enter the next NVS Camera Wizard screen.

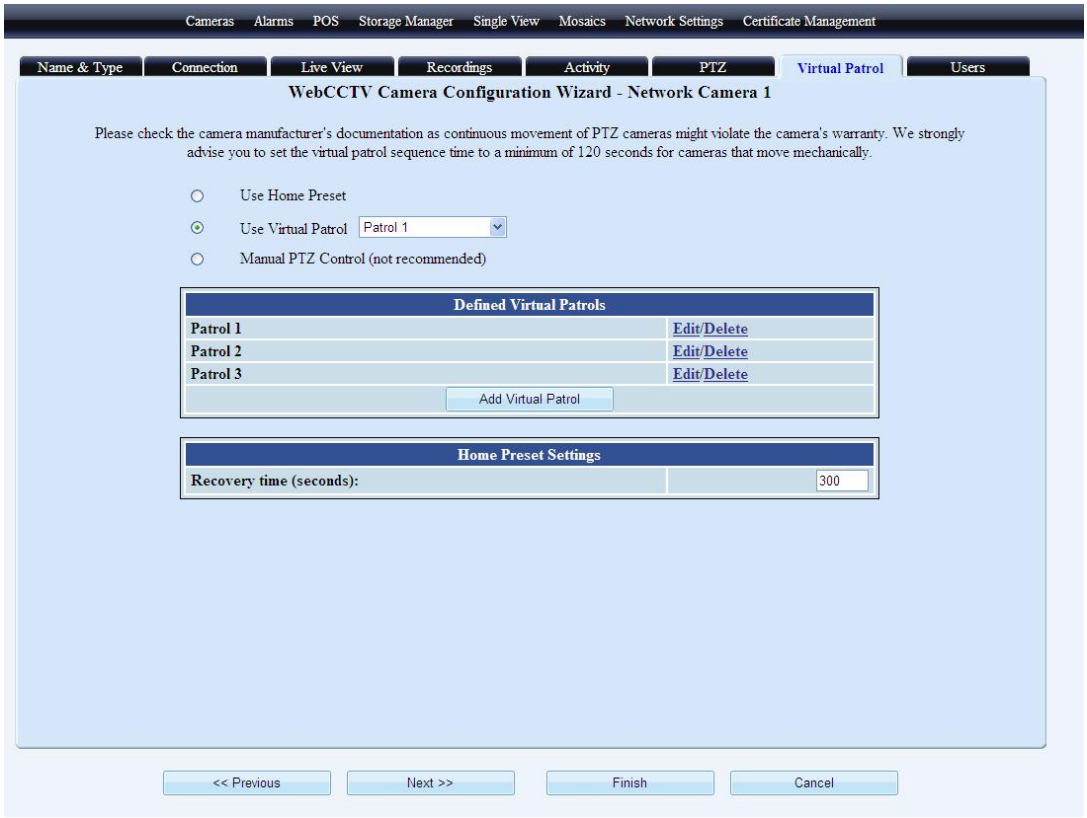
5.3.1.2.8 Virtual Patrol

This tab is a part of the **Network Video Server Camera Wizard**. The Virtual Patrol screen allows you to configure a PTZ camera in several ways:

- **Use Home preset** – this functionality prevents the misplacement of the camera and ensures proper recordings after monitoring. If the **Home Preset** is enabled, the first preset position becomes automatically the **Home** status and looks like in the **Live view**. When a user moves the PTZ camera, by manual manipulation or using preset positions, the camera will return to its Home Preset after the assigned **Recovery Time** has elapsed. By default this time is 300 seconds.

- **Use Virtual Patrol** – select one of the Virtual Patrol you previously created.

- **Manual PTZ Control** – check this radio button if you don't use either the Home Preset or the Virtual Patrol functionality.

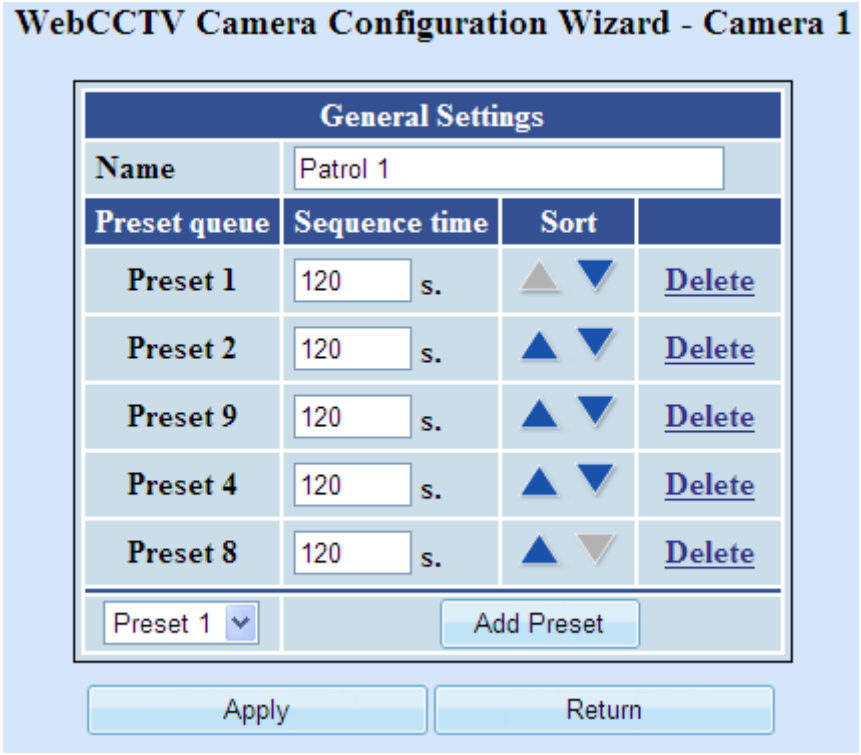


Virtual Patrol (Network Video Server) Screen

Only specially designed cameras designated by the manufacturer as "Continuous movement use", "Continuous duty cycle" or "24h duty cycle" can effectively utilize the Virtual Patrol feature. Using consumer-grade cameras with Virtual Patrol may cause premature failure and may invalidate the cameras warranty. We strongly advise customers to check the camera specifications before using the Virtual Patrol feature and strongly advise to set the virtual patrol sequence time to a minimum of 120 seconds for those cameras.

You can create multiple Virtual Patrols with different settings. Click the **Add Virtual Patrol** button to add a new Virtual Patrol.

To change or create the Virtual Patrol settings, click the **Edit** link.



Virtual Patrol Configuring Screen

1. Specify a **Name** for the Virtual Patrol.
2. Choose one of the available Presets from the drop-down list and click **Add Preset** button.
3. Specify the **Sequence time** for each Preset. This is the time after which the camera switches to the next defined preset in the queue.
4. If necessary, use the **Sort** buttons to change the position of a Preset in the Virtual Patrol sequence.
5. Click **Apply** button.

You may delete any Preset from the Virtual Patrol sequence by clicking the **Delete** link.

Due to some technology designs of Panasonic cameras it is recommended you use no more than 2-3 Panasonic cameras with virtual patrol configured at the same time, since this can cause server overloading.

Each time a user takes control over the PTZ camera manually (via the PTZ Camera Control Panel), the automatic Virtual Patrol is interrupted. Once the user stops his manual control, the WebCCTV resumes the Virtual Patrol after 30 seconds.

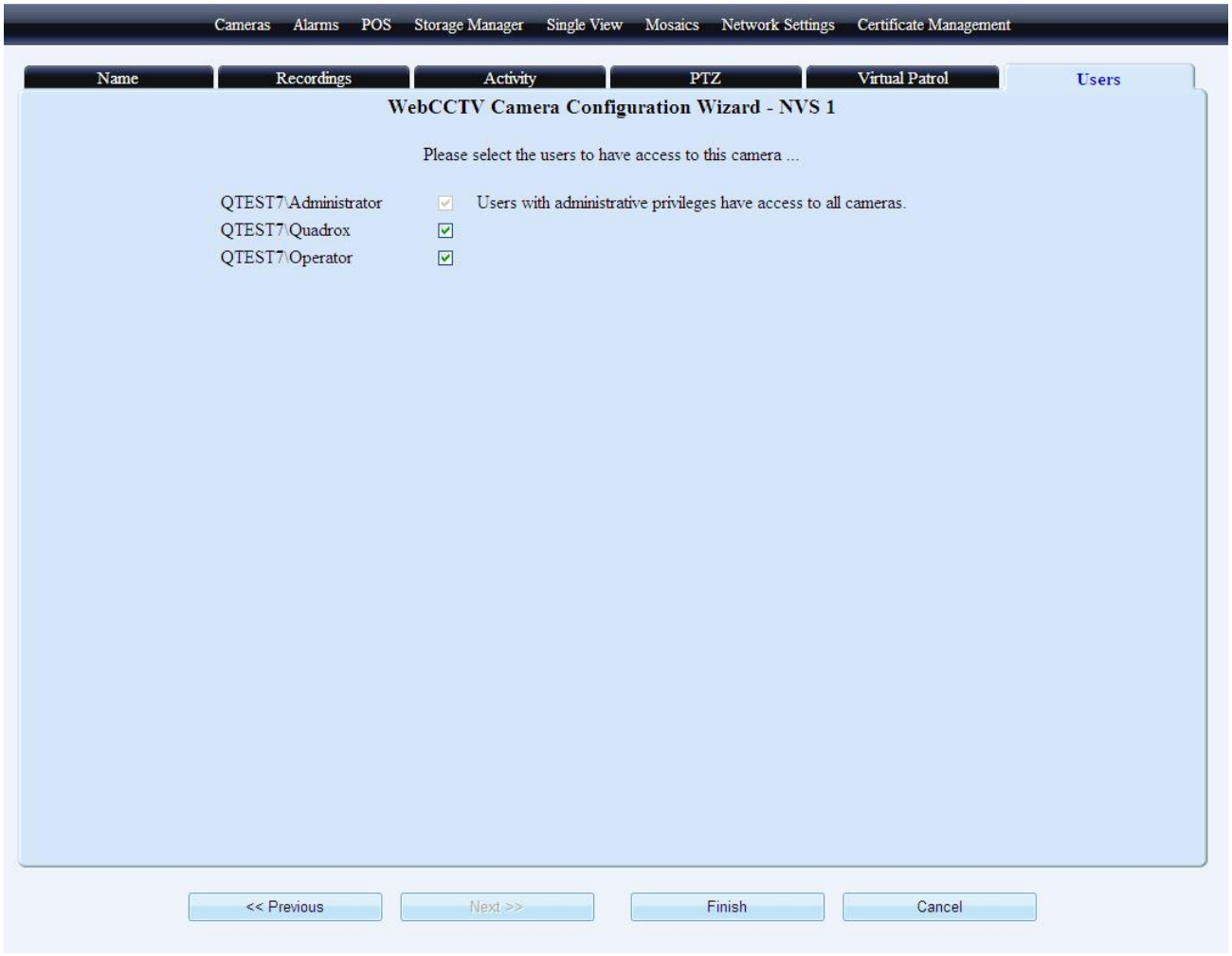
Click **Next** to enter the next NVS Camera Wizard screen.

5.3.1.2.9 Users

Select which users have access to the selected camera.

The Users functionality is only available after server restart when adding a new NVS. Follow the notification that automatically will be shown.

Users with Administrator rights have access to all the cameras. Users with restricted rights can be denied access to certain cameras.



Users (Network Video Server) Screen

5.3.2 Alarms

The **Alarms** chapter covers the handling and configuration of incoming alarms, alarm reactions and how to configure the actions linked to these incoming alarm events.

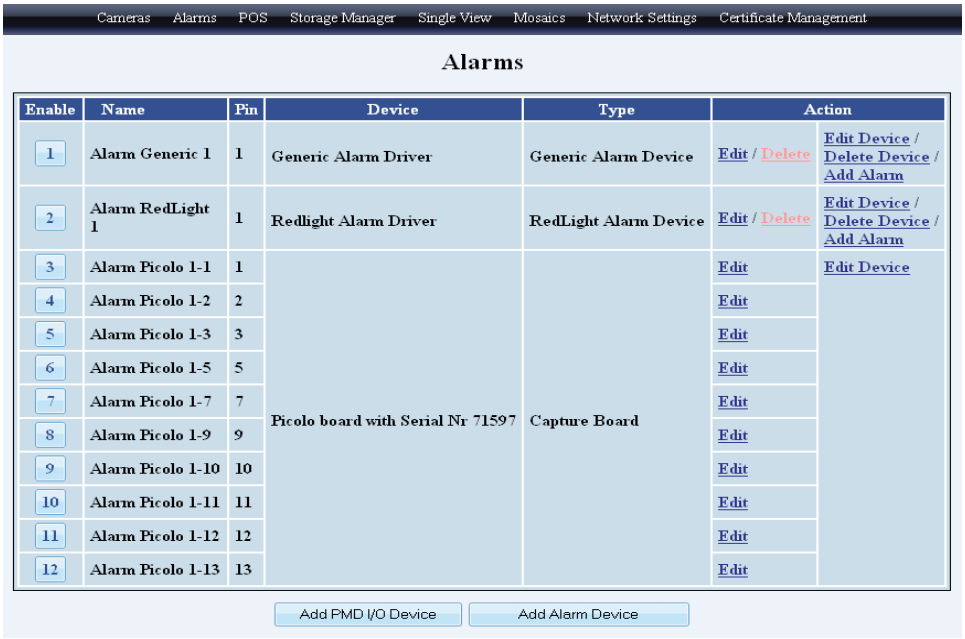
Input alarms can be generated through a physical alarm-input concentrator (screw-block to attach physical wires) attached on the back of the WebCCTV machine (together with a Picolo card), or through a PMD I/O Device (screw-block to attach physical wires) attached to the WebCCTV NVR via a USB cable.

The WebCCTV Alarm Component supports the OPC protocol; hence you are able to connect any OPC A&E compliant alarm server and OPC A&E compliant client as well to the WebCCTV Alarm Component. The origin of an alarm input can be an external infrared sensor, a reed contact, etc.

By default you get the alarms menu when clicking **Alarms** in the **Settings** menu. This menu allows you to **Add PMD I/O Device, Add Alarm Device** and access the Alarms Configuration Wizard by clicking **Edit** or **Edit Device**.

This chapter covers the following topics:

- Picolo I/O Proxy Device (Adding and Configuring)
- PMD I/O Device (Adding and Configuring)
- Generic Alarm Driver
- RedLight Driver
- Alarms Configuration Wizard


Cameras Alarms POS Storage Manager Single View Mosaics Network Settings Certificate Management
Alarms
Enable Name Pin Device Type Action
1 Alarm Generic 1 1 Generic Alarm Driver Generic Alarm Device Edit / Delete Edit Device / Delete Device / Add Alarm
2 Alarm RedLight 1 1 Redlight Alarm Driver RedLight Alarm Device Edit / Delete Edit Device / Delete Device / Add Alarm
3 Alarm Picolo 1-1 1 Picolo board with Serial Nr 71597 Capture Board Edit Edit Device
4 Alarm Picolo 1-2 2 Edit
5 Alarm Picolo 1-3 3 Edit
6 Alarm Picolo 1-5 5 Edit
7 Alarm Picolo 1-7 7 Edit
8 Alarm Picolo 1-9 9 Edit
9 Alarm Picolo 1-10 10 Edit
10 Alarm Picolo 1-11 11 Edit
11 Alarm Picolo 1-12 12 Edit
12 Alarm Picolo 1-13 13 Edit
Add PMD I/O Device
Add Alarm Device

Alarms Screen

5.3.2.1 Picolo I/O Proxy

When you start the WebCCTV server, it detects your Picolo I/O video capturing card and automatically sets it up.

WebCCTVs manufactured after 2007 may have a different type of capture card on which I/O is not supported. Use a PMD I/O Device in this case.

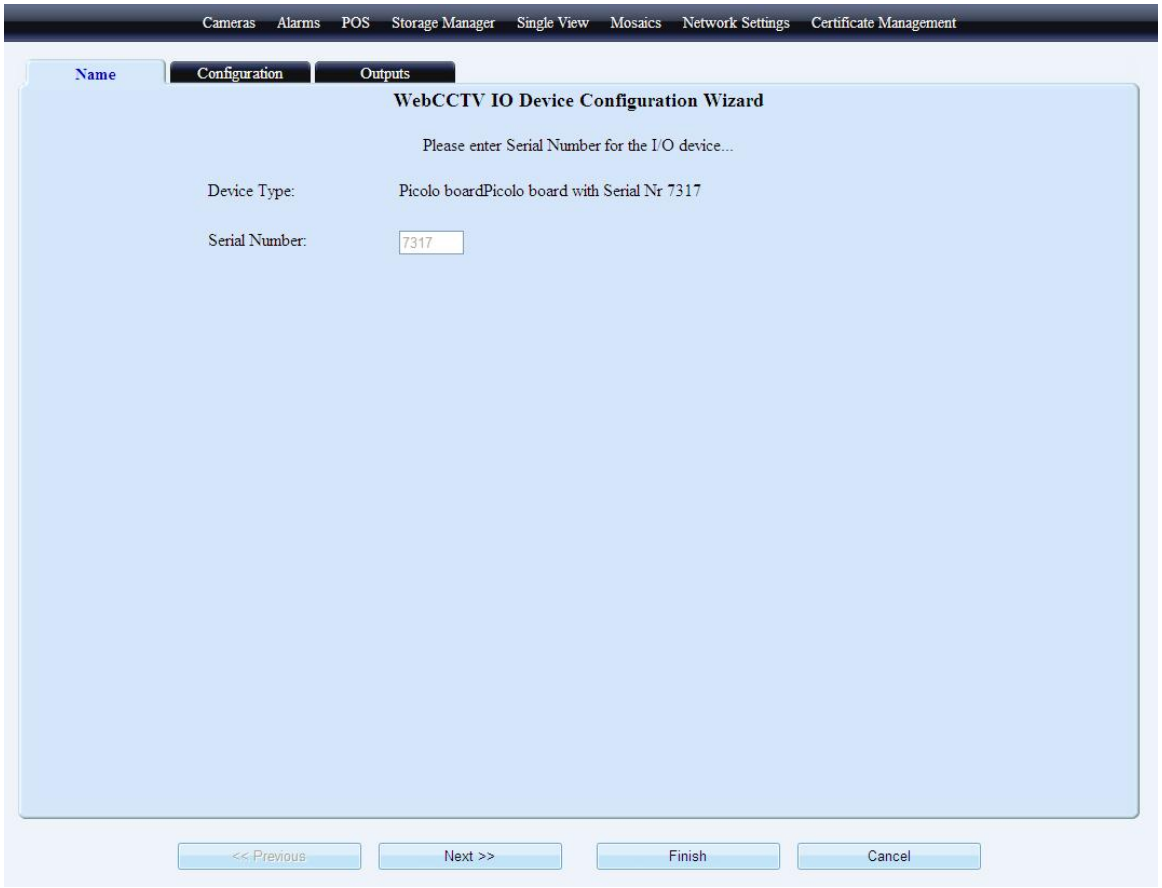
Alarms (Picolo I/O Proxy) Screen

Click the **Edit Device** link to open the **I/O Device Configuration Wizard** which allows for the configuration of the Picolo I/O Proxy.

5.3.2.1.1 Name

This screen doesn't allow you to configure any parameter. It contains two fields:

- **Device type** – general information about the type of I/O Device connected.
- **Serial Number** – serial number of your I/O Device.



Name (Picolo I/O Proxy) Screen

Click **Next** to enter the next I/O Device Configuration Wizard Screen.

5.3.2.1.2 Configuration

This screen allows you to configure your I/O Device lines as inputs or outputs for the alarm signals. If you don't need all of the line(s) you can disable the unused lines.

The screen contains the picture of the I/O Device connector with 13 drop-down lists around it which correspond to 13 lines of the I/O Device. Each drop-down list has 3 options available: **I, O** and **X.**

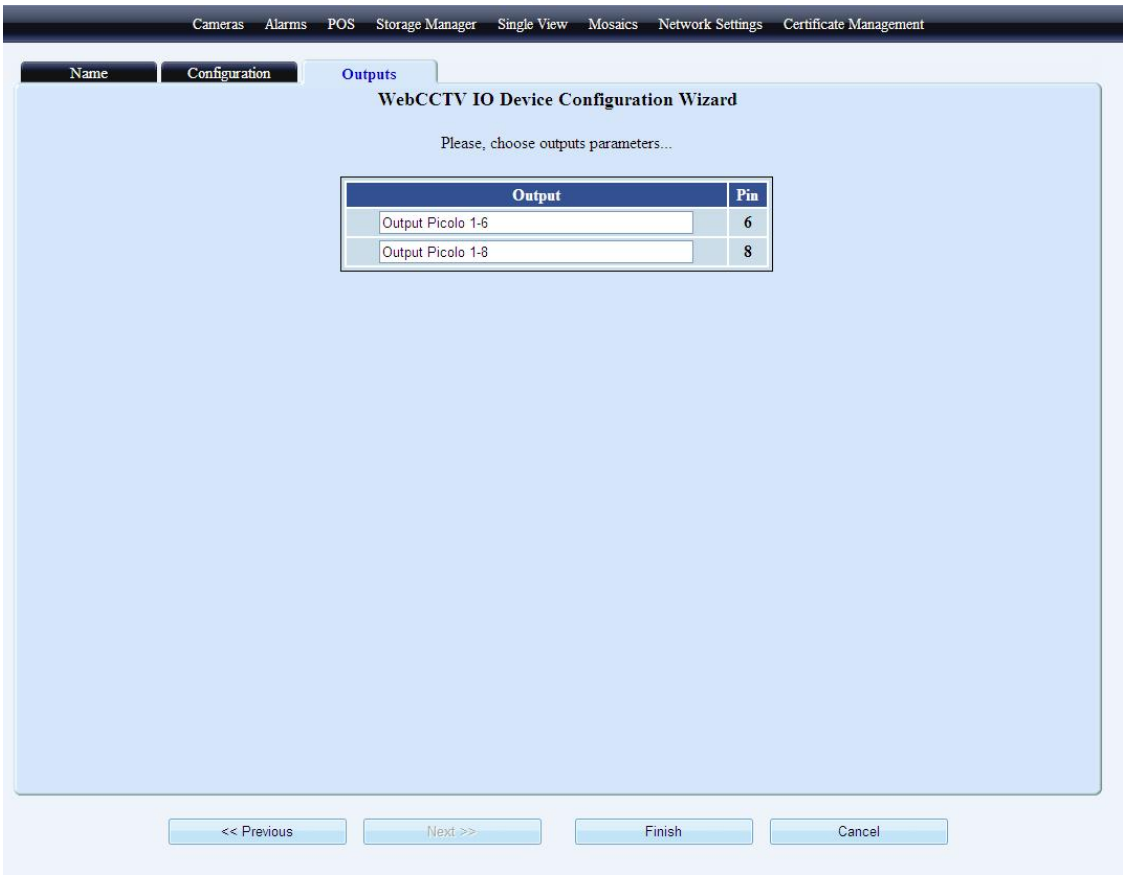
Configuration (Picolo I/O Proxy) Screen

Value	Description
I	Configure line as input. This line receives an alarm signal from an external device.
O	Configure line as output. This line sends a control signal to the external device.
X	Disable the line. This line neither receives, nor sends controls signals.

Click **Next** to enter the next I/O Device Configuration Wizard Screen.

5.3.2.1.3 Outputs

This screen allows you to assign names to the lines you have configured as outputs.



Outputs (Picolo I/O Proxy) Screen

If you didn't configure any line as an output, the following message will be shown: "**No outputs are currently configured for this device".** Consequently no configuration will be available on this page.

Click the **Finish** button to apply the configuration.

5.3.2.2 PMD I/O Device

The PMD I/O device has to be added manually. To do so, follow the steps below:

1. Attach the PMD I/O Device to one of the USB ports of your WebCCTV.

PMD I/O Device supports USB 2.0.

2. Click **Add PMD I/O Device** button.

Alarms (PMD I/O Device) Screen

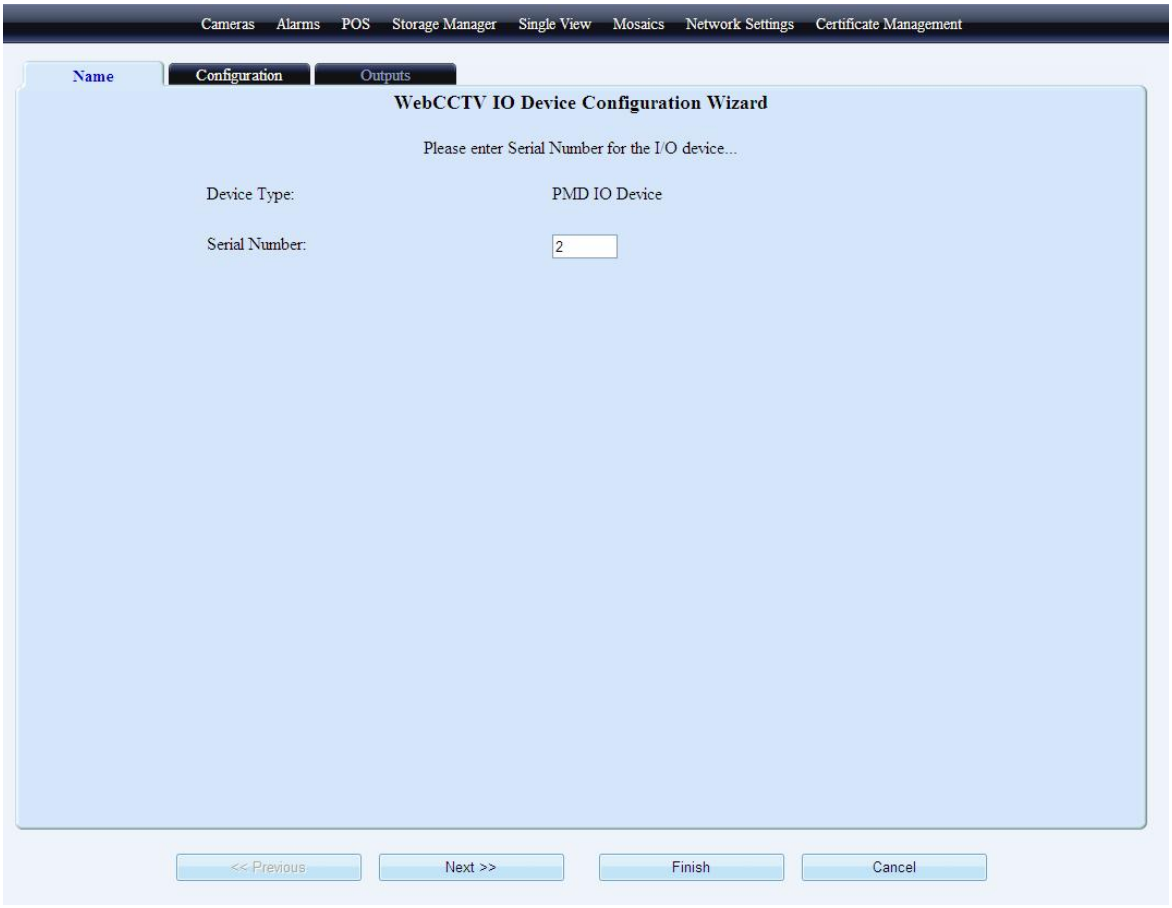
The **PMD I/O Device Configuration Wizard** will be opened for configuration.

5.3.2.2.1 Name

This screen shows basic information about the I/O Device. It contains two fields:

- **Device type** – general information about the type of I/O Device connected.
- **Serial Number** – enter the serial number of your I/O Device in this field.

To obtain the serial number of your PMD I/O Device, refer to PMD I/O Device documentation or use the special tool that is located in the Support folder to set a new serial number. (see ***3.3.2.2.5 PMD I/O Serial Number***)

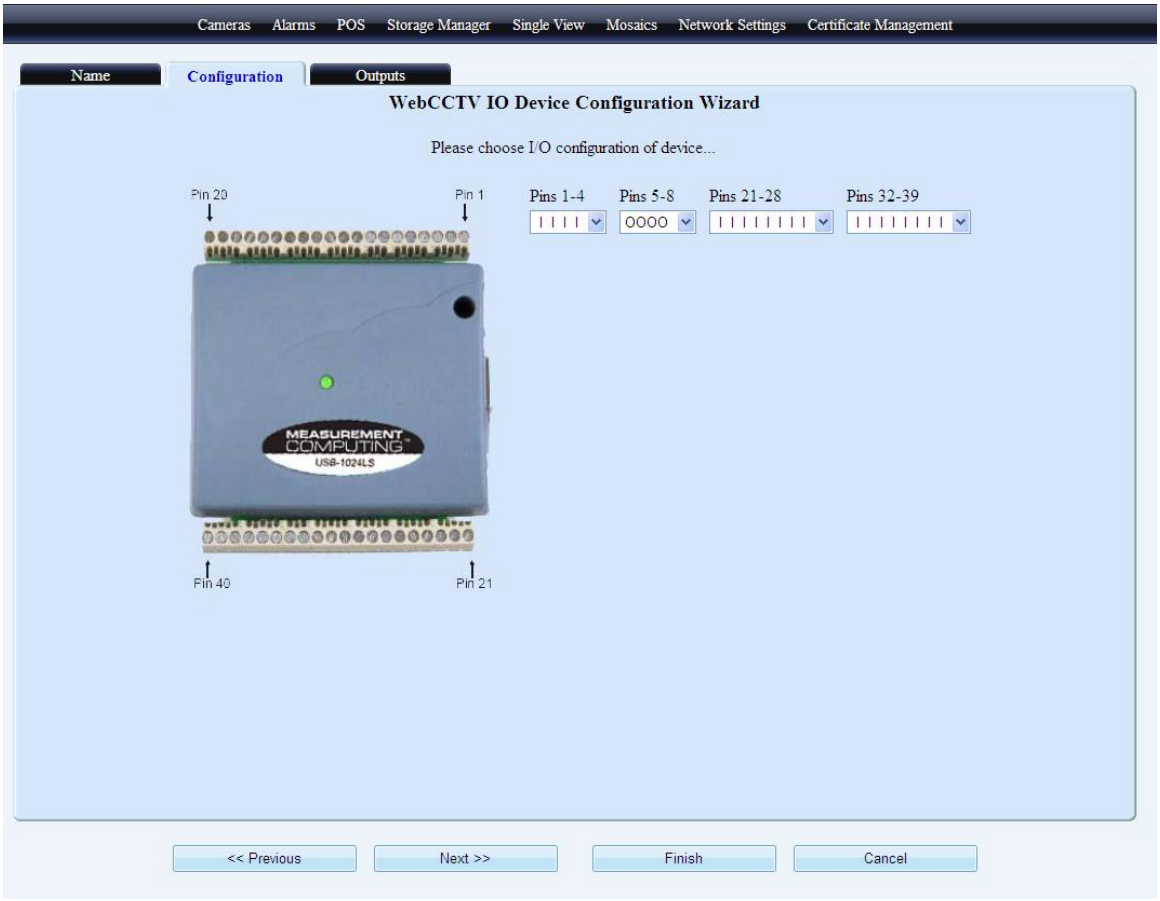


Name (PMD I/O Device) Screen

Click **Next** to enter the next I/O Device Configuration Wizard Screen.

5.3.2.2.2 Configuration

This screen allows you to configure your I/O Device lines as inputs or outputs for the alarm signals.



Configuration (PMD I/O Device) Screen

When the PMD I/O device is disconnected from the USB port and the server is restarting, the PMD device disappears from I/O Devices list. After being reconnected and subsequently restarting the server, it appears again.

The PMD I/O device has 3 ports and each port has 8 lines, however one port is divided in two parts, where every subpart has 4 lines. This makes 24 lines in total. Compared to the Picolo I/O card, where every line can be configured separately, you need to configure a whole port as an input or output for the PMD I/O device. There are 4 drop-down lists and each of them corresponds to a certain port.

Value	Description
I	Configure line as input. This line receives an alarm signal from an external device.
O	Configure line as output. This line sends a control signal to the external device.

Click the **Finish** button**.**

If you entered a correct PMD I/O Device serial number you should see the following screen:

Cameras Alarms POS Storage Manager Single View Mosaics Network Settings Certificate Management
Alarms
I/O Device was successfully added
Enable Name Pin Device Type Action
1 Alarm PMD 1-1 1 PMD with Serial Nr 2 PMD USB Device Edit Edit Device Delete Device
2 Alarm PMD 1-2 2 Edit
3 Alarm PMD 1-3 3 Edit
4 Alarm PMD 1-4 4 Edit
5 Alarm PMD 1-9 9 Edit
6 Alarm PMD 1-10 10 Edit
7 Alarm PMD 1-11 11 Edit
8 Alarm PMD 1-12 12 Edit
9 Alarm PMD 1-13 13 Edit
10 Alarm PMD 1-14 14 Edit
11 Alarm PMD 1-15 15 Edit
12 Alarm PMD 1-16 16 Edit
13 Alarm PMD 1-17 17 Edit
14 Alarm PMD 1-18 18 Edit

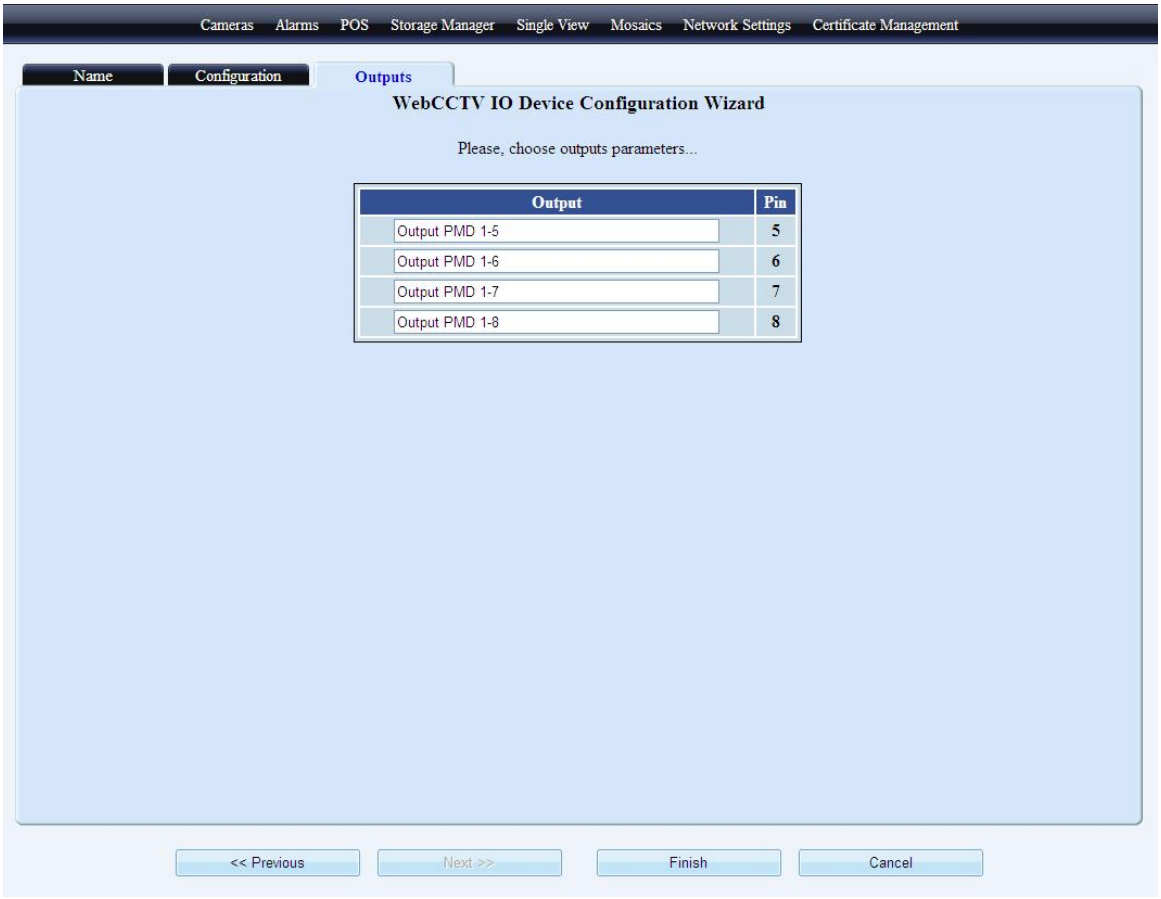
Alarms (PMD I/O Device Added) Screen

Click the **Edit Device** link. Go to the **Outputs** tab.

5.3.2.2.3 Outputs

This screen allows you to assign names to the lines you have configured as outputs.

The **Outputs** tab is not available in the WebCCTV PMD I/O Device Configuration Wizard when you are adding the PMD I/O Device. It becomes available after you have added the device and click **Edit Device** link in the Alarms menu.



Outputs (PMD I/O Device) Screen

Click the **Finish** button to apply the configuration.

5.3.2.2.4 Delete PMD I/O Device

If you want to delete your PMD I/O Device, execute the following steps:

1. While being in the Alarms Menu, click the **Delete Device** link.

Cameras
Alarms
POS
Storage Manager
Single View
Mosaics
Network Settings
Certificate Management
Alarms
Enable
Name
Pin
Device
Type
Action
1 Alarm PMD 1-1 1 Edit Edit Device Delete Device
2 Alarm PMD 1-2 2 Edit
3 Alarm PMD 1-3 3 Edit
4 Alarm PMD 1-4 4 Edit
5 Alarm PMD 1-9 9 Edit
6 Alarm PMD 1-10 10 Edit
7 Alarm PMD 1-11 11 Edit
8 Alarm PMD 1-12 12 Edit
9 Alarm PMD 1-13 13 Edit
10 Alarm PMD 1-14 14 Edit
11 Alarm PMD 1-15 15 PMD with Serial Nr 2 PMD USB Device Edit
12 Alarm PMD 1-16 16 Edit
13 Alarm PMD 1-17 17 Edit
14 Alarm PMD 1-18 18 Edit

Alarms (Deleting PMD I/O Device) Screen

2. Click **OK** in the pop-up window.

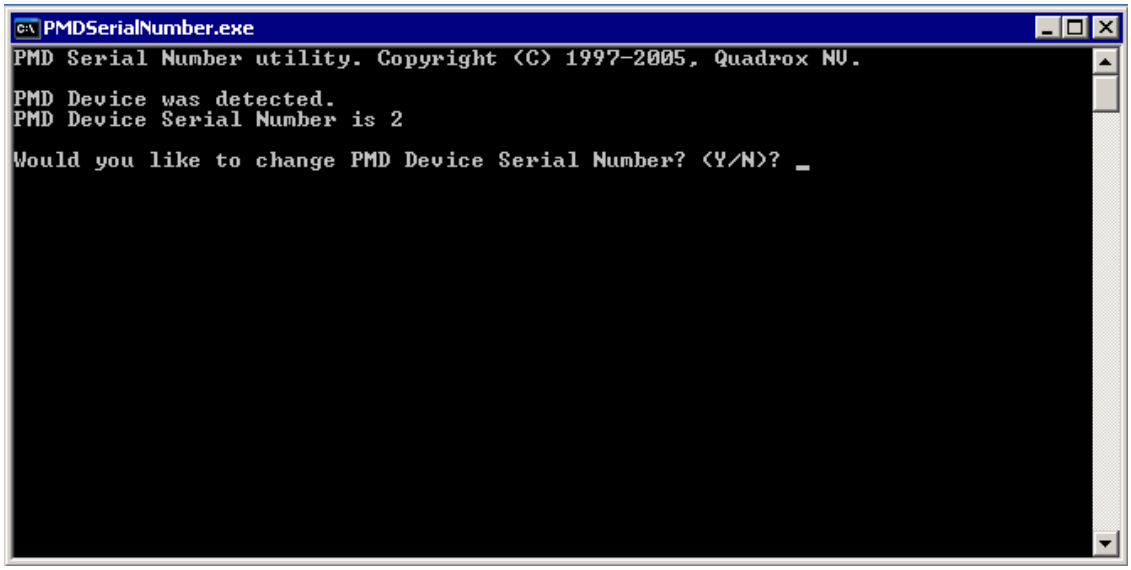
Windows Internet Explorer
This operation will cause your alarm configuration to be reset.
Are you sure that you want to delete this device?
OK
Cancel

Confirmation (Deleting PMD I/O Device) Screen

5.3.2.2.5 PMD I/O serial number

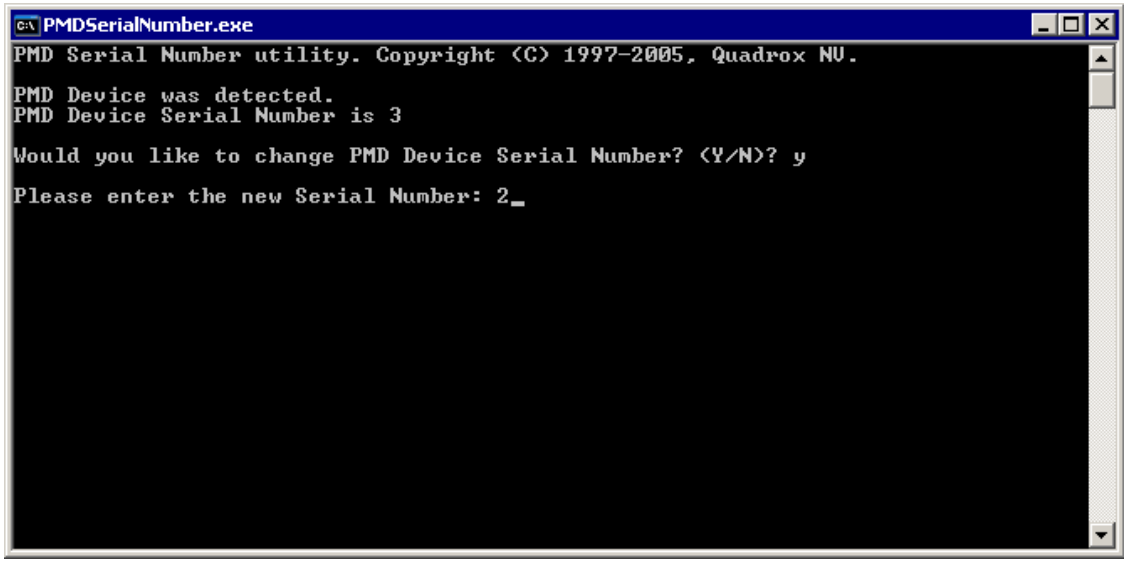
To assign the serial number to a PMD I/O Device, follow the steps below:

1. Connect your PMD I/O Device to the computer.
2. Go to **C:\Program Files\Quadrox**, find **pmdserialnumber.exe** and click on it.
3. A command prompt will appear.


PMDSerialNumber.exe
PMD Serial Number utility. Copyright (C) 1997-2005, Quadrox NV.
PMD Device was detected.
PMD Device Serial Number is 2
Would you like to change PMD Device Serial Number? (Y/N)?

Assigning PMD I/O Serial Number Screen 1

4. Specify **Y** and click **Enter** button.
5. The message **'Please enter the new serial number'** will appear on the screen. Specify the new serial number. Click **Enter**.


PMDSerialNumber.exe
PMD Serial Number utility. Copyright (C) 1997-2005, Quadrox NV.
PMD Device was detected.
PMD Device Serial Number is 3
Would you like to change PMD Device Serial Number? (Y/N)? y
Please enter the new Serial Number: 2

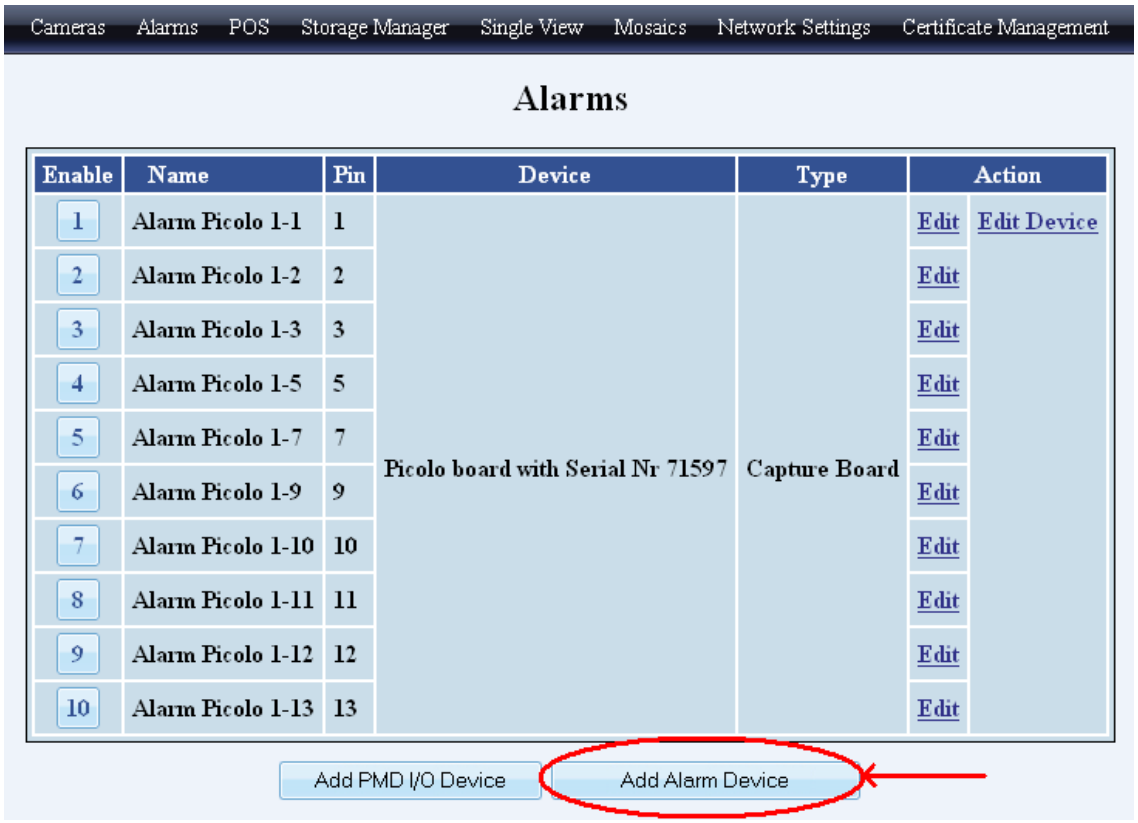
Assigning PMD I/O Serial Number Screen 2

6. As prompted, press any key to finish assigning the PMD I/O Device serial number.

5.3.2.3 Generic Alarm Driver

The Generic Alarm Driver makes it possible to generate alarms without needing a hardware device. Generating alarms is done by using the SDK (Software Development Kit). For more information about how to utilize the SDK Kit, contact SDK@quadrox.be.

To add the Generic Alarm Driver, click **Add Alarm Device** button.

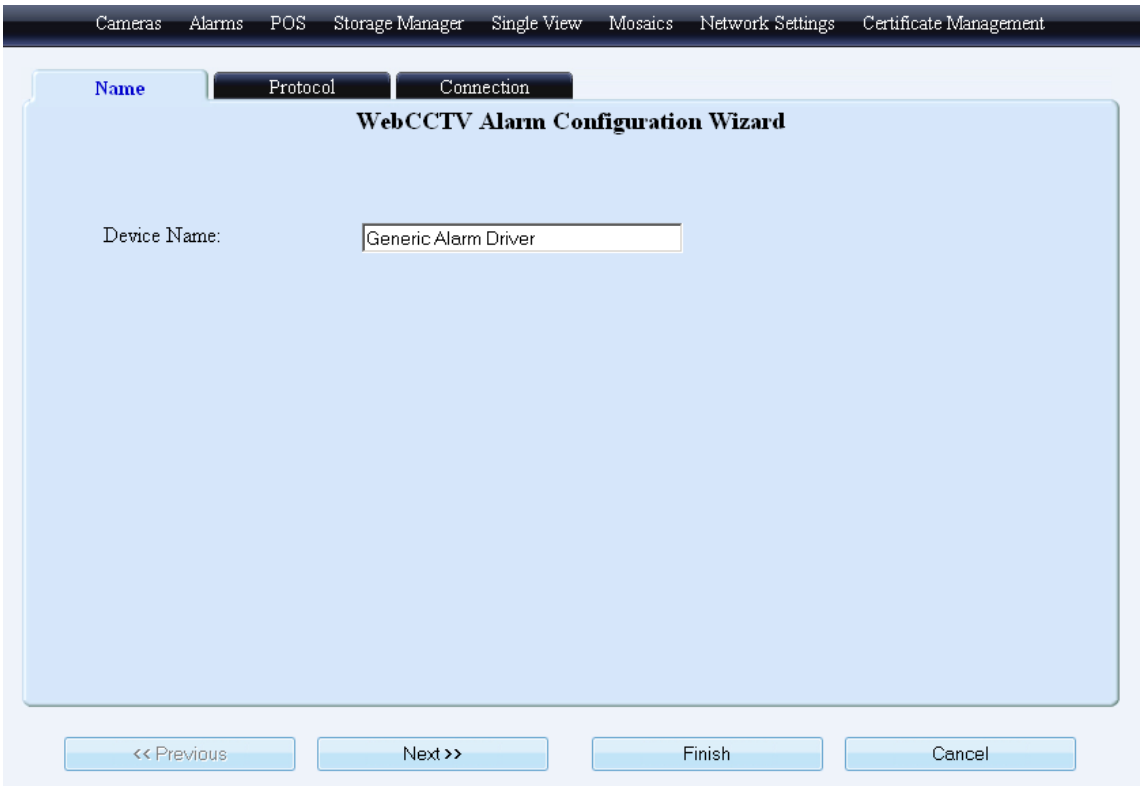


Alarms Screen

The **Alarm Configuration Wizard** will be opened for configuration.

5.3.2.3.1 Name

This tab allows you to specify the **Device Name**.



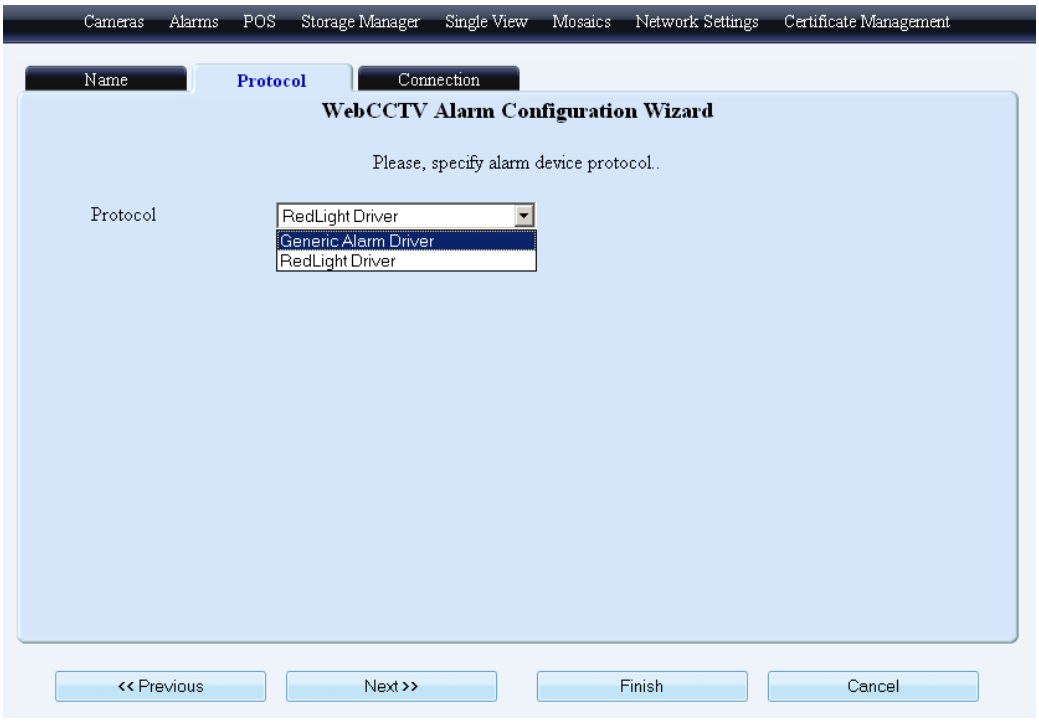
Name (Generic Alarm Driver) Screen

Click **Next** to enter the next Alarm Configuration Wizard Screen.

5.3.2.3.2 Protocol

In this tab, the protocol has to be selected.

Select **Generic Alarm Driver** in the drop-down list.



Protocol (Generic Alarm Driver) Screen

Click the **Finish** button.

Depending on the drivers you installed together with the Alarm Component, it's possible that some values are not present in the drop-down list.

If you entered the Alarm Configuration Wizard by clicking the **Edit Device** link in the Alarms Screen, you can't change the protocol anymore, but you can only see which protocol has been selected.

5.3.2.3.3 Connection

This tab is not available for the Generic Alarm Driver Device. You don't have to configure it.

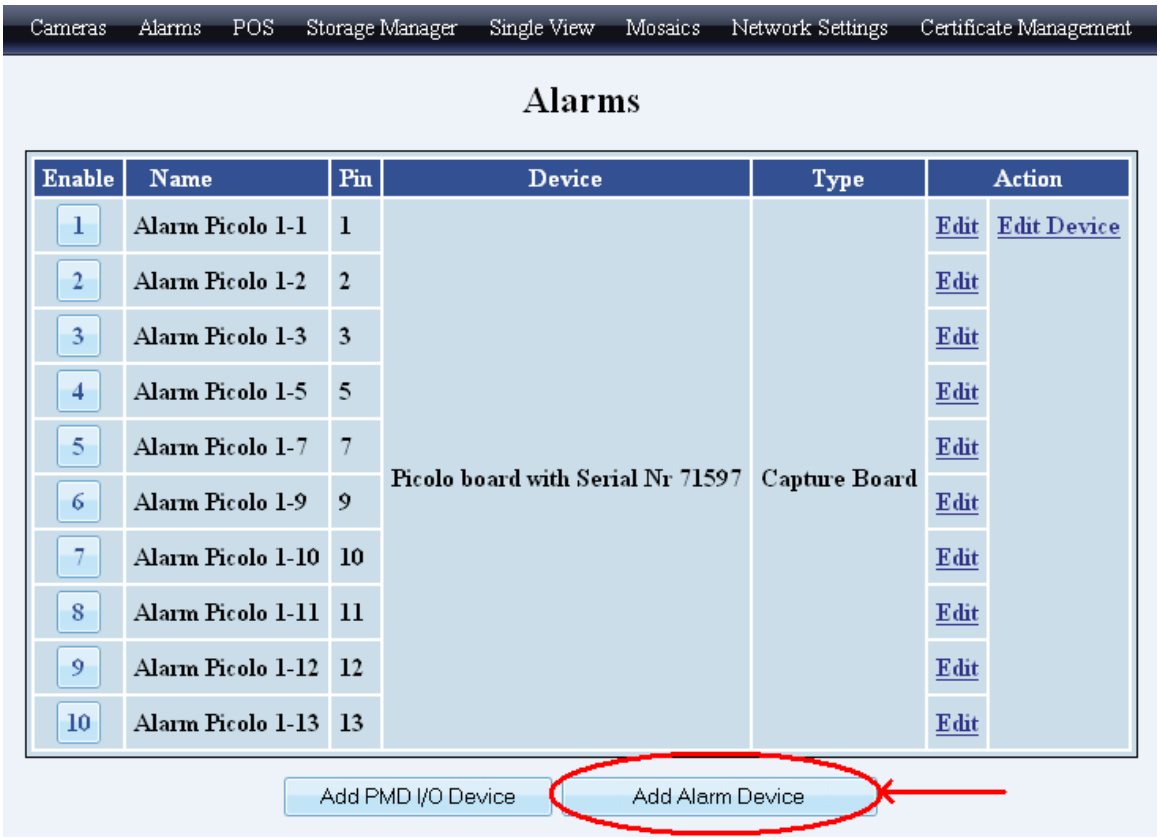
5.3.2.4 RedLight Alarm Driver

The RedLight Alarm Driver makes it possible to receive alarms for Red Light infractions.

This driver may and can only be used in cooperation with Quadrox N.V. For more information, contact sales@quadrox.be.

You need extra add-on software to be able to receive alarms.

To add the RedLight Alarm Driver, click **Add Alarm Device** button.

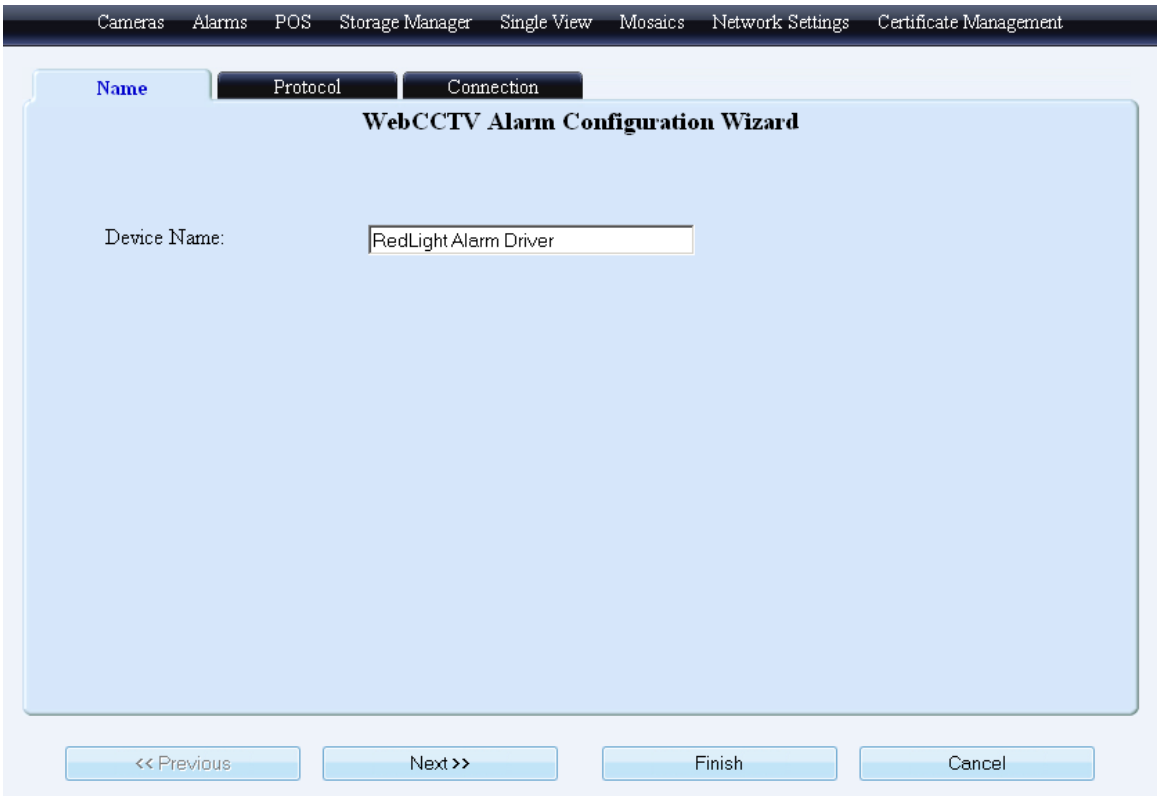


Alarms Screen

The **Alarm Configuration Wizard** will be opened for configuration.

5.3.2.4.1 Name

This tab allows you to specify the **Device Name**.



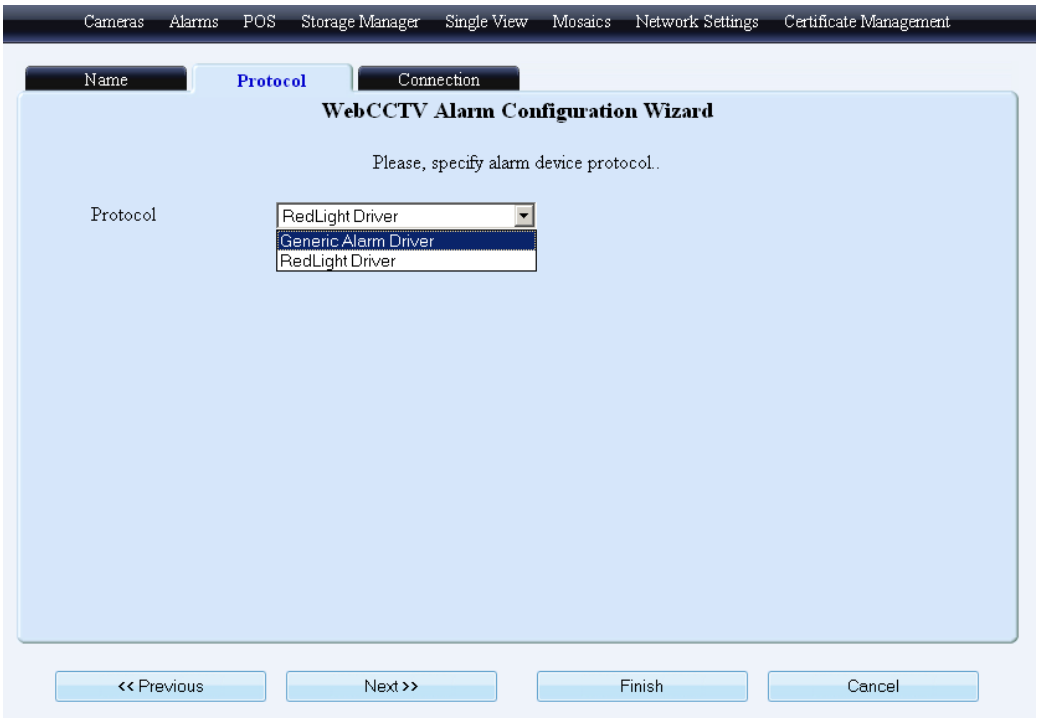
Name (RedLight Alarm Driver) Screen

Click **Next** to enter the next Alarm Configuration Wizard Screen.

5.3.2.4.2 Protocol

In this tab, the protocol has to be selected.

Select **RedLight Driver** in the drop-down list.



Protocol (RedLight Alarm Driver) Screen

Click **Next** to enter the next Alarm Configuration Wizard Screen.

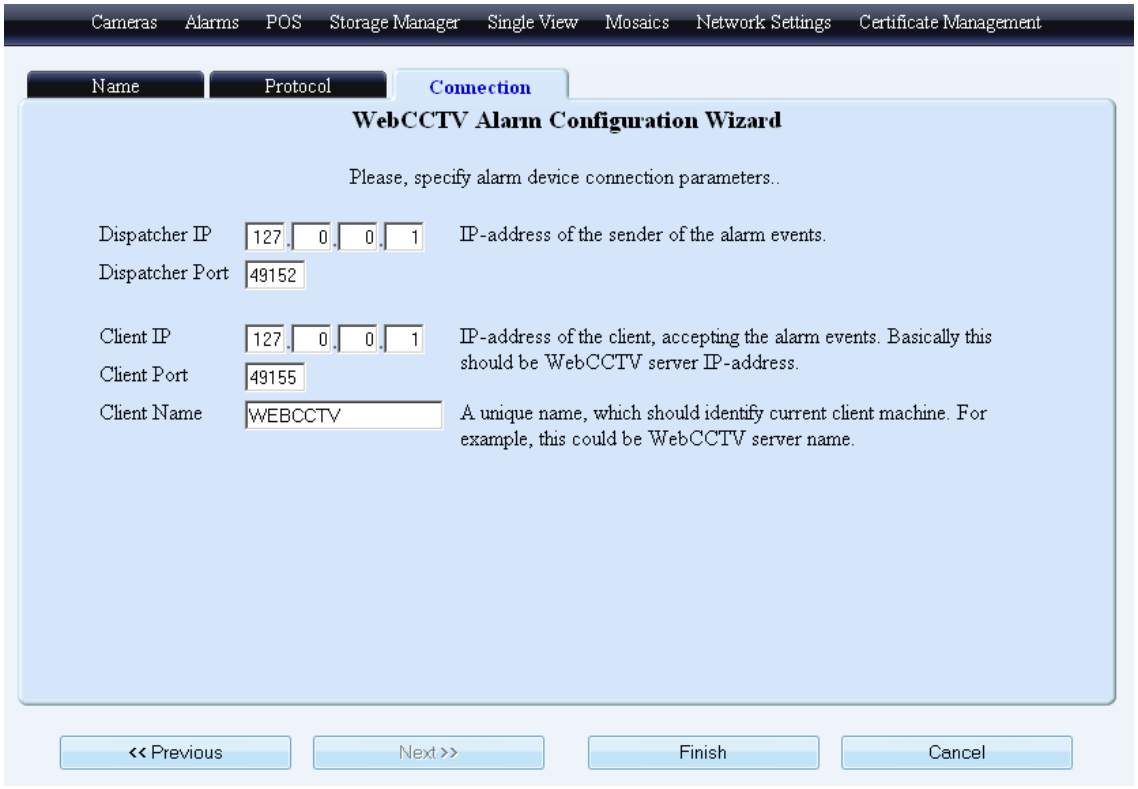
Depending on the drivers you installed together with the Alarm Component, it's possible that some values are not present in the drop-down list.

If you entered the Alarm Configuration Wizard by clicking the **Edit Device** link in the Alarms Screen, you can't change the protocol anymore, but you can only see which protocol has been selected.

5.3.2.4.3 Connection

This tab allows the configuration of the following settings:

- **Dispatcher IP** – IP address of the sender of the alarm events.
- **Dispatcher Port** – port used by the dispatcher to send alarm events.
- **Client IP** – IP address of the client which accepts the alarm events. Basically this should be the WebCCTV server IP Address.
- **Client Port** – port used by the client to receive alarm events.
- **Client Name** – unique name which identifies the client machine.



Connection (RedLight Alarm Driver) Screen

5.3.2.5 Alarm Configuration Wizard

To enter the Alarm Configuration Wizard in order to configure the alarms itself, click one of the **Edit** links in the Alarms Menu. The Alarm Configuration Wizard consists of eight tabs with easy to follow instructions. Read this chapter to learn all about the alarms configuration.

The following Alarm Configuration Wizard tabs are described in this chapter:

- Name
- PTZ
- Recordings
- FTP
- Outputs
- Notification
- Mail
- SMS

By default, some of the settings are already selected. It is recommended you keep these settings to ensure the best performance.

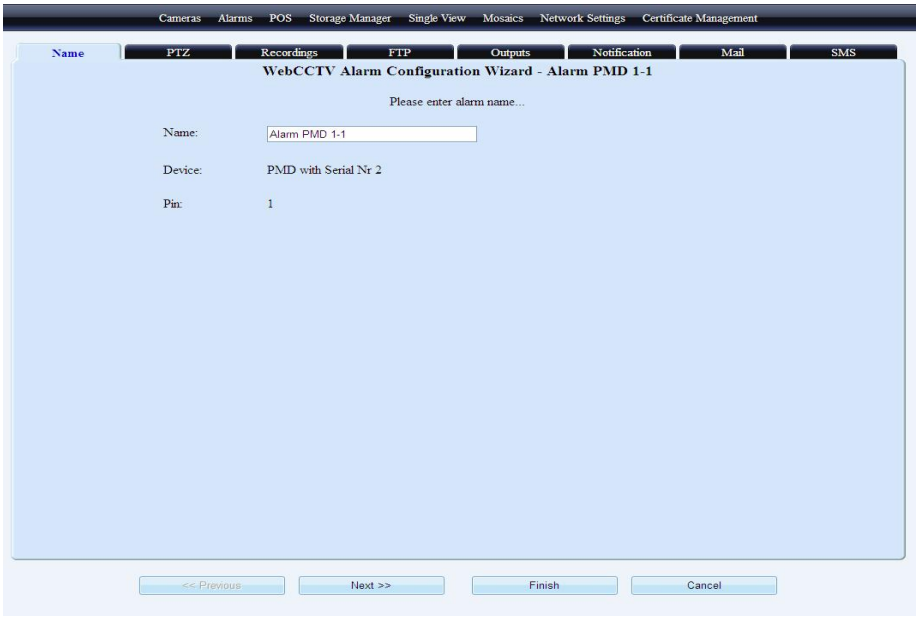
When configuring a hybrid WebCCTV, you are able to use 13 Input/Output lines (for Q16 model – 26 I/O lines if 2 Picolo Tetra cards are used) by means of Picolo I/O Proxy. A PMD I/O Device gives you the ability to use 24 Input/Output lines. WebCCTVs manufactured after 2007 may have a different type of capture card on which I/O is not supported. Use a PMD I/O Device in this case.

A PMD I/O Device or Picolo I/O Proxy Device has a fixed amount of alarms available. For the RedLight and Generic Device, you can add as many alarms as you wish by clicking the **Add Alarm** link in the Alarms Screen.

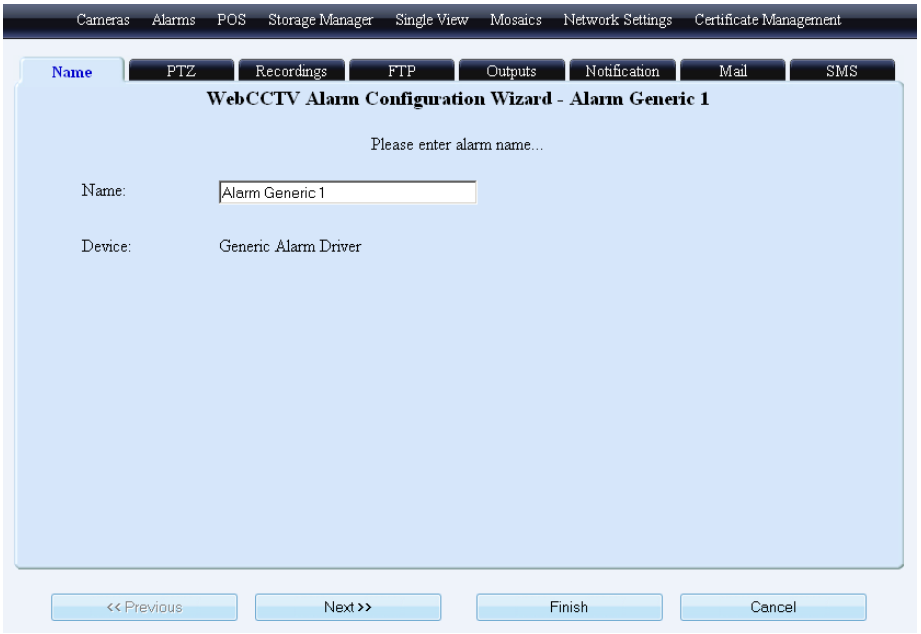
5.3.2.5.1 Name

In this tab, you can define the alarm name and see the device and pin to which the alarm is associated.

Choose a descriptive name for each alarm for future reference.



Name (Alarm – PMD I/O Device) Screen



Name (Alarm – Generic / RedLight Alarm Driver) Screen

Click **Next** to enter the next Alarm Configuration Wizard Screen.

5.3.2.5.2 PTZ

You can choose the PTZ reaction for the incoming alarm, meaning if an alarm is triggered the specified camera will turn to the selected camera preset position. To configure this feature, follow the steps below:

1. Select the camera from the drop-down list.
2. Select the preferred preset position.
3. Click the **Add camera** button.

You are able to change the preset position for the camera only after it has been added. Settings presets is explained in the Video Browser manual.

If there are no PTZ camera configured in the system, the message "No PTZ cameras are available in the system" will be shown.

PTZ (Alarm) Screen

To delete the camera, click **Delete**.

Click **Next** to enter the next Alarm Configuration Wizard Screen.

5.3.2.5.3 Recordings

In this tab you are able to do the following:

- Add or delete cameras to record when an alarm occurs.

Multiple recordings can be assigned to one alarm. This way, an incident can be monitored from different cameras and angles.

- Set the recording time before and after an alarm has occurred. This is also called the pre and post alarm recording interval.

An alarm movie is labelled recorded footage from a camera you attached to the alarm, i.e. when an alarm comes in, the specific period of time recorded from a specified camera is labelled and saved. Once the recording is complete, it appears as an alarm movie. If there aren't any recordings (i.e. when there is no activity) for the period when the alarm occurs, you won't have an alarm movie. You can set a camera to record all the time via the Camera Configuration Wizard.

To add the camera to be recorded when an alarm is triggered, follow the steps below:

1. Select the camera from the drop-down list.
2. Select the pre and post alarm label interval for each camera.
3. Click the **Add camera** button.

Recordings (Alarm) Screen

To delete a camera, click **Delete**.

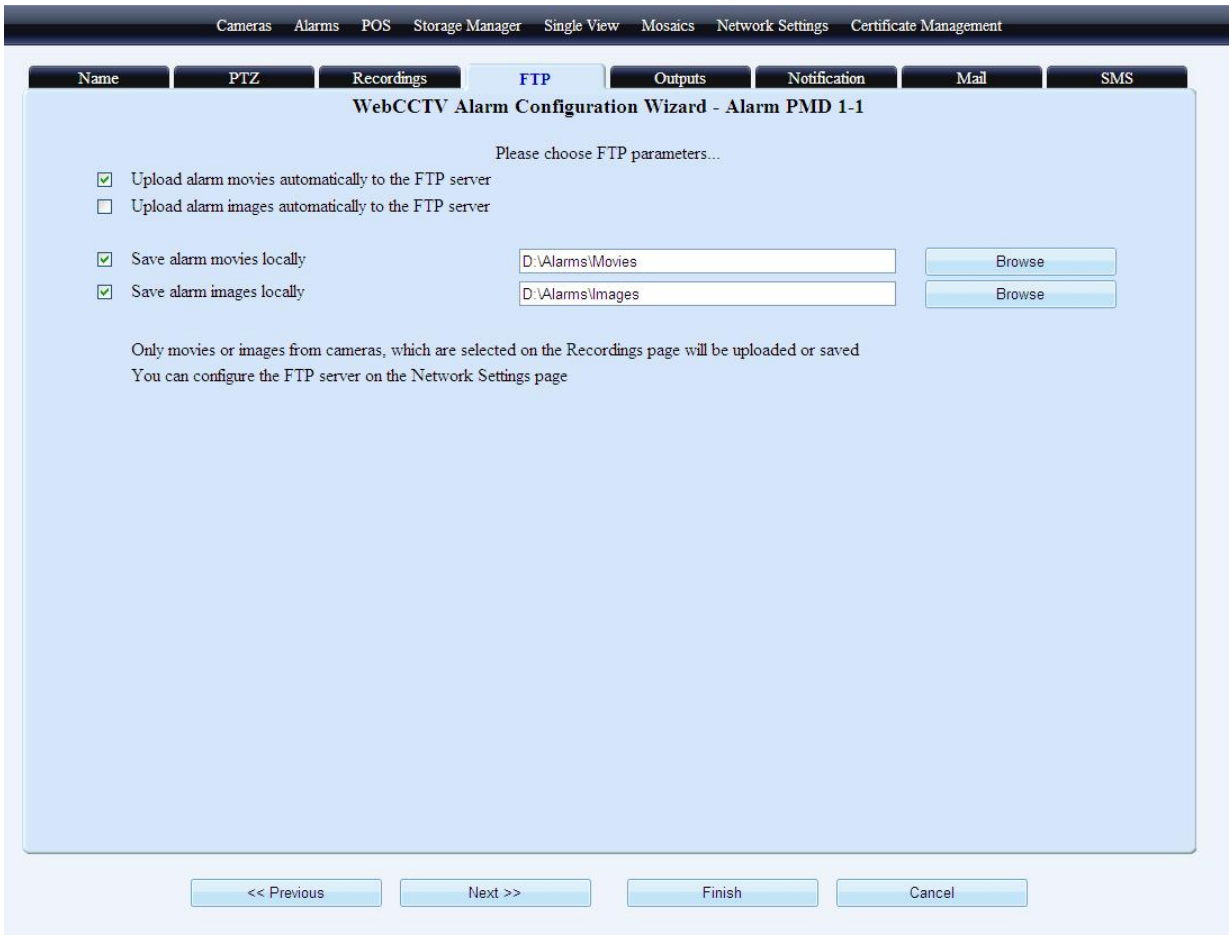
Click **Next** to enter the next Alarm Configuration Wizard Screen.

5.3.2.5.4 FTP

The FTP upload function enables automatic uploading of the movies and images, which were created based on an incoming alarm, onto a remote FTP server or to a local folder for further revision and storing. To configure FTP uploading, see ***3.3.7.2 FTP Parameters***.

An alarm image is a snapshot captured at the moment the alarm is triggered.

To use this feature, select the corresponding checkbox.



FTP (Alarm) Screen

Click **Next** to enter the next Alarm Configuration Wizard Screen.

5.3.2.5.5 Outputs

This tab allows you to configure which outputs will send the signals to the external devices when an alarm is triggered.

The output tab is only available if some lines of the I/O device are set as output.

To configure outputs follow the steps below:

1. Select the output from the corresponding drop – down list.
2. Select the state to which the output will switch when an alarm is triggered.

By default the output is in Low State. This means that the voltage on the corresponding pin is 0 V. When an alarm is triggered, the output switches to the High State which corresponds to the voltage of 5 V.

3. Choose when the output will return to its previous state. There are two variants:

   - Output returns to its previous state in a time span you indicate.
   - Output returns to its previous state on the deactivation of the triggered alarm.

4. Click the **Add Output** button.

Outputs (Alarm) Screen

Click **Next** to enter the next Alarm Configuration Wizard Screen.

5.3.2.5.6 Notification

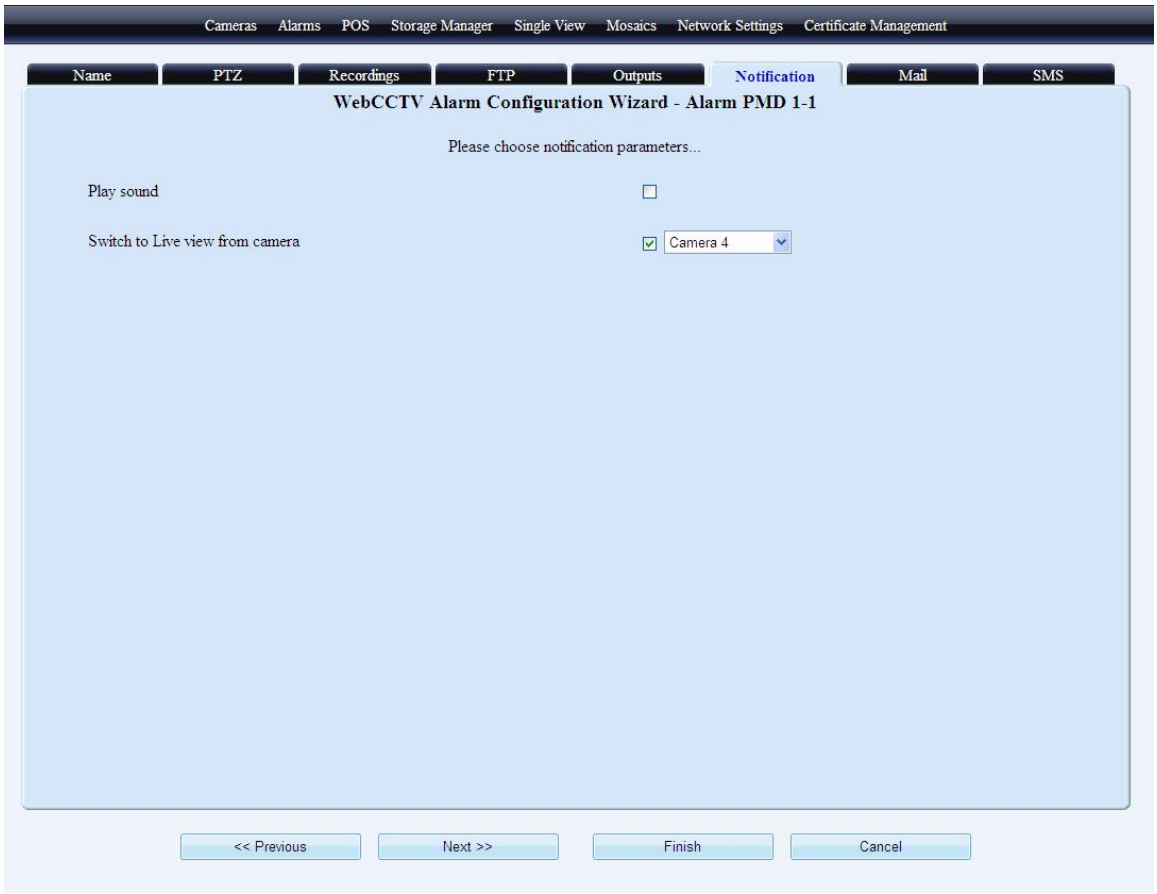
This tab allows you to configure the sound notification for an incoming alarm. At the same time, it's possible to automatically switch to live view for an assigned camera.

To use the sound notification, speakers should be connected to the WebCCTV server.

To get the sound notification signal when an alarm is triggered, select the **Play sound** checkbox.

To configure switching to Live View on a specific camera, follow the steps below:

1. Select **Switch to Live view from camera** checkbox.
2. Choose the desired camera from the drop-down list.



Notification (Alarm) Screen

Click **Next** to enter the next Alarm Configuration Wizard Screen.

5.3.2.5.7 Mail

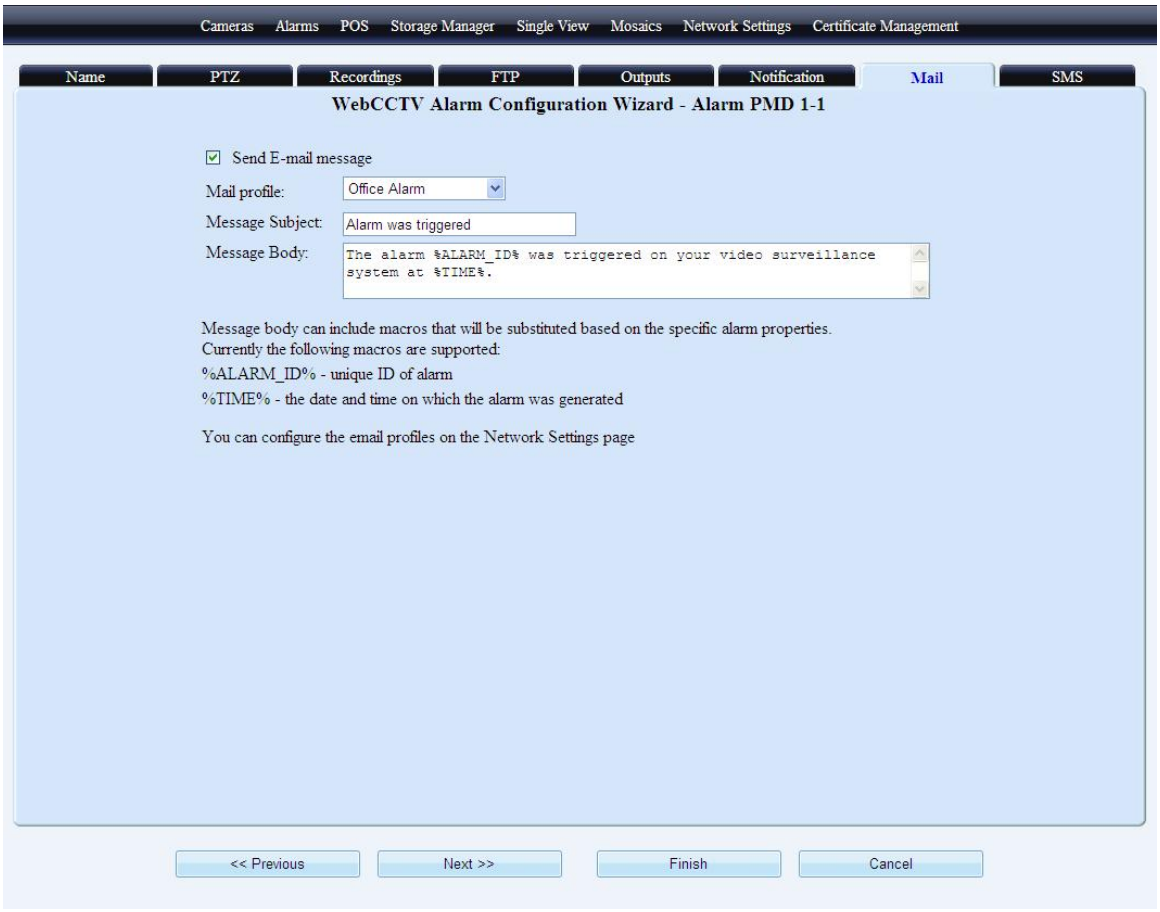
This tab allows you to configure an email notification when an alarm is triggered. It means that you will be sent an e-mail giving you the basic information about the triggered alarm (by default). In order to activate the email notification feature, follow the steps below:

1. Select the **Send E-Mail Message** checkbox.
2. Select a mail profile from the drop-down list.

To create a mail profile, see ***3.3.7.4 E-Mail Profile***.

3. Specify the **Message Subject** and **Message Body** in the corresponding fields. The message body can include macros that will be substituted based on the specific alarm properties. Following macros are supported:

   - **%ALARM_ID%** – unique ID of the alarm.
   - **%TIME%** – date and time on which the alarm was generated.



Mail (Alarm) Screen

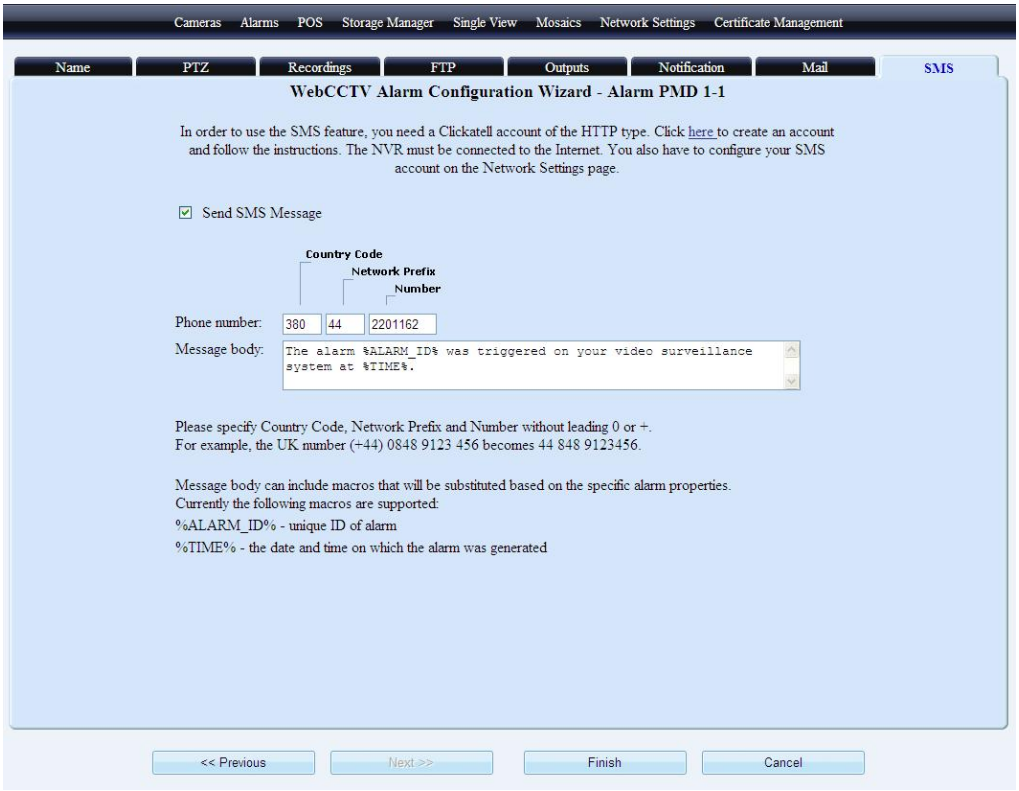
Click **Next** to enter the next Alarm Configuration Wizard Screen.

5.3.2.5.8 SMS

This tab allows you to configure an SMS notification when an alarm is triggered. It means that you will be sent a SMS message giving you the basic information about the triggered alarm (by default).

You need a Clickatell account to use the SMS notification feature. Use the direct link http://www.clickatell.com/developers/api_http.php or use the link on the SMS page in order to create an account.

To configure your SMS account, see ***3.3.7.3 SMS Account Parameters.***


Cameras
Alarms
POS
Storage Manager
Single View
Mosaics
Network Settings
Certificate Management
Name
PTZ
Recordings
FTP
Outputs
Notification
Mail
SMS
WebCCTV Alarm Configuration Wizard - Alarm PMD 1-1
In order to use the SMS feature, you need a Clickatell account of the HTTP type. Click here to create an account and follow the instructions. The NVR must be connected to the Internet. You also have to configure your SMS account on the Network Settings page.
Send SMS Message
Country Code
Network Prefix
Number
Phone number:
380
44
2201162
Message body:
The alarm %ALARM_ID% was triggered on your video surveillance system at %TIME%.
Please specify Country Code, Network Prefix and Number without leading 0 or +.
For example, the UK number (+44) 0848 9123 456 becomes 44 848 9123456.
Message body can include macros that will be substituted based on the specific alarm properties.
Currently the following macros are supported:
%ALARM_ID% - unique ID of alarm
%TIME% - the date and time on which the alarm was generated
<< Previous
Next >>
Finish
Cancel

SMS (Alarm) Screen

In order to use the SMS Notification feature, execute the following steps:

1. Check the **Send SMS Message** checkbox.
2. Enter the phone number you would like the SMS message to be sent to. Don't put the leading + or 00 when specifying the Country Code.
3. Edit the default or create a new message body text in a **Message Body** textbox. The message body can include macros that will be substituted based on the specific alarm properties. Following macros are supported:

    - **%ALARM_ID%** – unique ID of the alarm
    - **%TIME%** – date and time on which the alarm was generated

Click **Finish** to apply the settings.

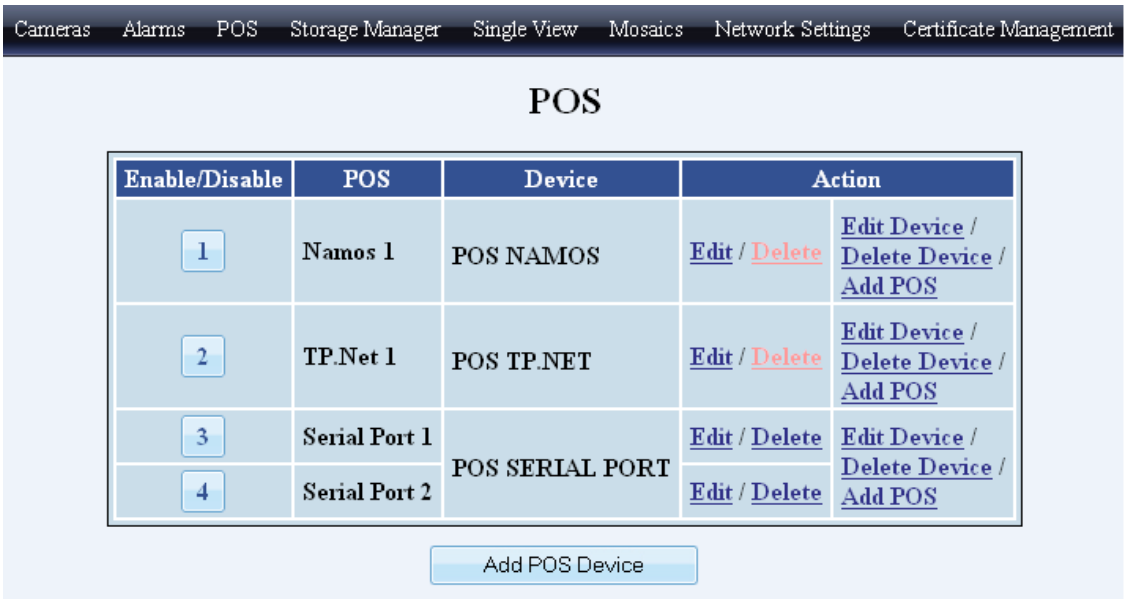
5.3.3 POS

This chapter explains how to configure the WebCCTV POS (**Point of Sale**) functionality. The POS functionality is a part of the WebCCTV Alarm Component. It transforms POS printer transactions into WebCCTV alarms. In other words, when a ticket is generated by the POS terminal, an alarm is triggered within WebCCTV. This makes it possible to observe all transactions and recordings which are recorded based on the incoming transaction data into the WebCCTV system.

The following POS types (devices) are supported in WebCCTV:

- Serial Port POS
- Generic POS
- TP.Net
- NAMOS

The POS device and its sources have to be added in WebCCTV in order to let WebCCTV process the incoming POS ticket information.



POS Screen

To enter the POS Device Configuration Wizard, click the **Edit device** or **Add POS Device** link/button in the POS screen. The **POS Device Configuration Wizard** consists of four tabs with easy to follow instructions.

The following **POS Device Configuration Wizard** tabs are described in the corresponding subchapters of Serial Port POS, TP.Net and NAMOS:

- Name
- Protocol
- Connection
- Storage

After you added a Serial Port POS Device, you have to add a POS printer by adding it as a source.

To configure or add POS sources, click the **Edit** or **Add POS** link in the POS screen which will lead you to the POS configuration Wizard. The **POS Configuration Wizard** consists of two tabs with easy to follow instructions.

When a POS device is added, the first POS source is added by default.

You can add several POS Sources (POS Printers) to a single POS Device.

The following **POS Configuration Wizard** tabs are described in the corresponding subchapters of Serial Port POS, TP.Net and NAMOS:

- Name
- Recordings

The POS functionality is a part of the WebCCTV Alarm Component. You need the Alarm Component installed before you can use the POS functionality.

When installing the Alarm Component, the Serial Port POS and Generic POS driver is installed by default. If you need the TP.Net or NAMOS driver, you need to select them in the custom menu which is available when installing the Alarm Component.

To delete a POS Device or source, click the **Delete** link.

5.3.3.1 Serial Port POS

Before you can add and configure a Serial Port POS Device and sources in WebCCTV, you need to:

1. Connect the POS printer you want to control by means of WebCCTV to the serial port (COM port) of any computer in your network.
2. Install the **Remote POS Monitor** application on this computer and configure it. (See ***3.3.3.1.1 Remote POS Monitor***)

When all steps are completed, Remote POS Monitor will capture the transactions that come from the POS printer which is connected to the COM port and will send them to the WebCCTV server.

In order to add and configure your POS device, click the **Edit device** or **Add POS Device** link/button in the POS screen. The **POS Device Configuration Wizard** consists of four tabs with easy to follow instructions.

In order to configure the sources, click the **Edit** link of the source in the POS screen which will lead you to the POS configuration Wizard. The **POS Configuration Wizard** consists of two tabs with easy to follow instructions.

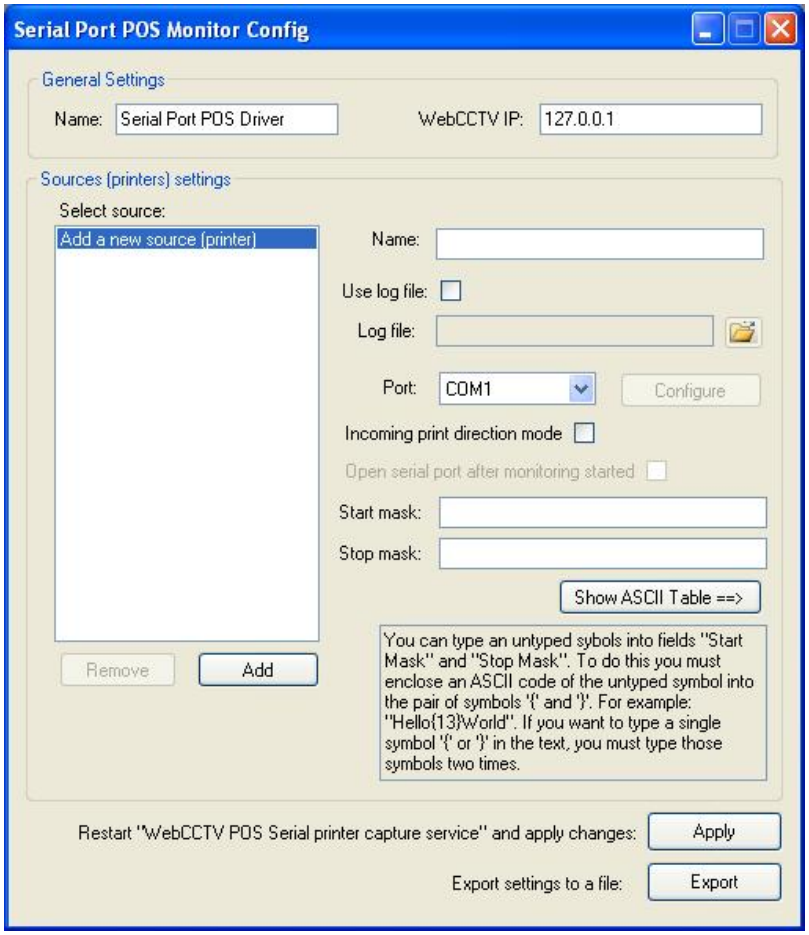
The POS functionality is a part of the WebCCTV Alarm Component. You need to have the Alarm Component installed before you can use the POS functionality.

5.3.3.1.1 Remote POS Monitor

Remote POS Monitor is needed for capturing the transactions coming from the POS printer connected to the COM port which sends them to the WebCCTV server.

First you need to install Remote POS Monitor on the computer by running the installation file which can be found on the Alarm Component CD, called: "**RemotePOSMonitorSetup.exe**".

After the installation, open the Configuration Application by going to **Start -> All Programs -> Remote POS Monitor -> Configuration Application**. A window will open:


Serial Port POS Monitor Config
General Settings
Name: Serial Port POS Driver
WebCCTV IP: 127.0.0.1
Sources (printers) settings
Select source:
Add a new source (printer)
Name:
Use log file:
Log file:
Port: COM1
Configure
Incoming print direction mode
Open serial port after monitoring started
Start mask:
Stop mask:
Show ASCII Table ==>
You can type an untyped sybols into fields "Start Mask" and "Stop Mask". To do this you must enclose an ASCII code of the untyped symbol into the pair of symbols '{' and '}'. For example: "Hello{13}World". If you want to type a single symbol '{' or '}' in the text, you must type those symbols two times.
Remove
Add
Restart "WebCCTV POS Serial printer capture service" and apply changes:
Apply
Export settings to a file:
Export

POS Monitor Configuration Screen

You are able to add the POS printer(s) (sources) to be monitored by means of this configuration tool. To do this, follow the steps below:

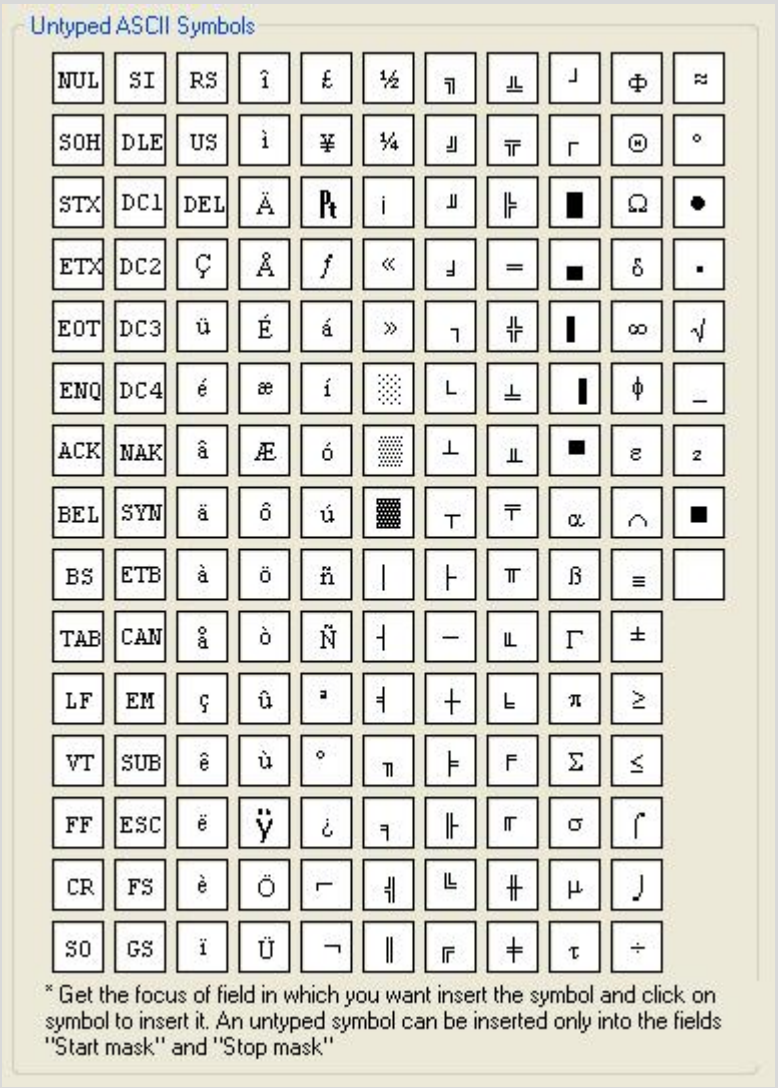
1. Specify the IP address of the WebCCTV server in the **WebCCTV IP** field to connect the POS Monitor to the server.

If the WebCCTV server is installed on the same machine the POS printer is connected to, do not use the 127.0.0.1 IP address, but fill in the real IP-address. You can check the real IP address in the TCP/IP properties of your machine.

2. Select the **Add a new source (printer)…** item in the list of POS printers (sources).

3. Specify the name of the POS printer you want to add in the **Name** field.
4. Select the **COM port** to which the printer is connected.
5. Specify the **Start Mask**. Start Mask is the expression or the number of symbols by which the POS printer ticket is started. This information is needed for POS Monitor to recognize the beginning of a ticket and send it to the WebCCTV server for further proceeding.
6. Specify the **Stop Mask**. Stop Mask is the expression or the number of symbols by which the POS printer ticket is finished. This information is needed for POS Monitor to recognize the end of a ticket and send it to the WebCCTV server for further proceeding.

If the **Start mask** or **Stop mask** of the ticket has nonprinting symbols (symbols which are not represented on a keyboard but can be present in the POS ticket), please select the corresponding symbol after putting your cursor in the start or stop mask field. The corresponding decimal value will become visible in the start or stop mask. Click the **Show ASCII Table** button to show the **ASCII Table:**


Untyped ASCII Symbols
NUL SI RS
SOH DLE US
STX DC1 DEL
ETX DC2
EOT DC3
ENQ DC4
ACK NAK
BEL SYN
BS ETB
TAB CAN
LF EM
VT SUB
FF ESC
CR FS
SO GS
* Get the focus of field in which you want insert the symbol and click on symbol to insert it. An untyped symbol can be inserted only into the fields "Start mask" and "Stop mask"

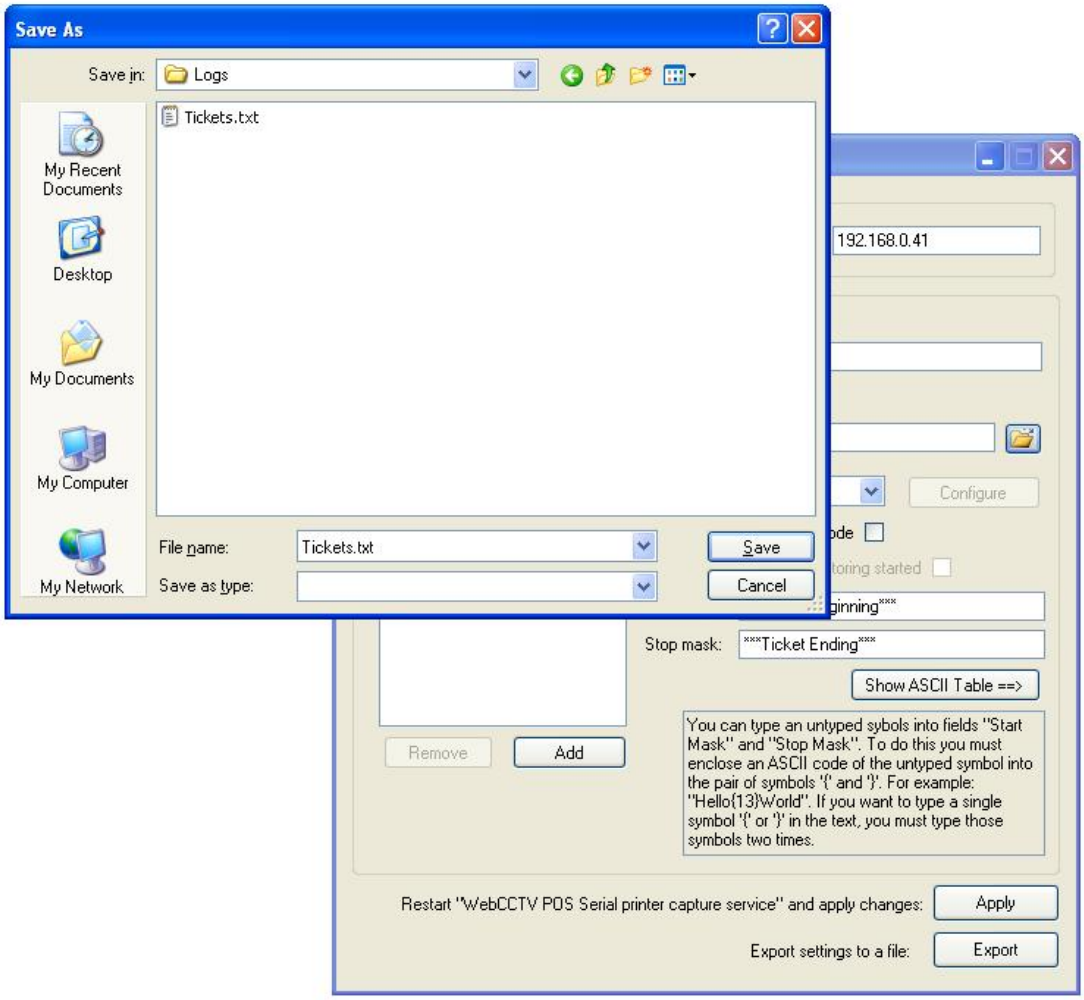
Use the following rule when specifying the nonprinting symbols:

- Enclose an ASCII decimal code of the corresponding nonprinting symbol into the

pair of symbols **{ }**. For example: **Hello{168}World** means **Hello¿ World**

- If you want to specify a single symbol { or }, specify these symbols two times. For example: **{{Hello World}}** means **{Hello World}**

7. If you want to see the information inside the tickets coming from the POS printer to the COM port, check the **Use log file** checkbox. Choose/create the log file the information will be written to and click **Save**.


Save As
Save in:
Logs
Tickets.txt
My Recent Documents
Desktop
My Documents
My Computer
My Network
File name:
Tickets.txt
Save as type:
Save
Cancel
192.168.0.41
Configure
Stop mask:
Ticket Ending
Show ASCII Table ==>
You can type an untyped sybols into fields "Start Mask" and "Stop Mask". To do this you must enclose an ASCII code of the untyped symbol into the pair of symbols '{' and '}'. For example: "Hello{13}World". If you want to type a single symbol '{' or '}' in the text, you must type those symbols two times.
Remove
Add
Restart "WebCCTV POS Serial printer capture service" and apply changes:
Apply
Export settings to a file:
Export

Selecting a Log File Screen

Now each ticket which comes from the POS printer will be written to the log file **Tickets.txt.**

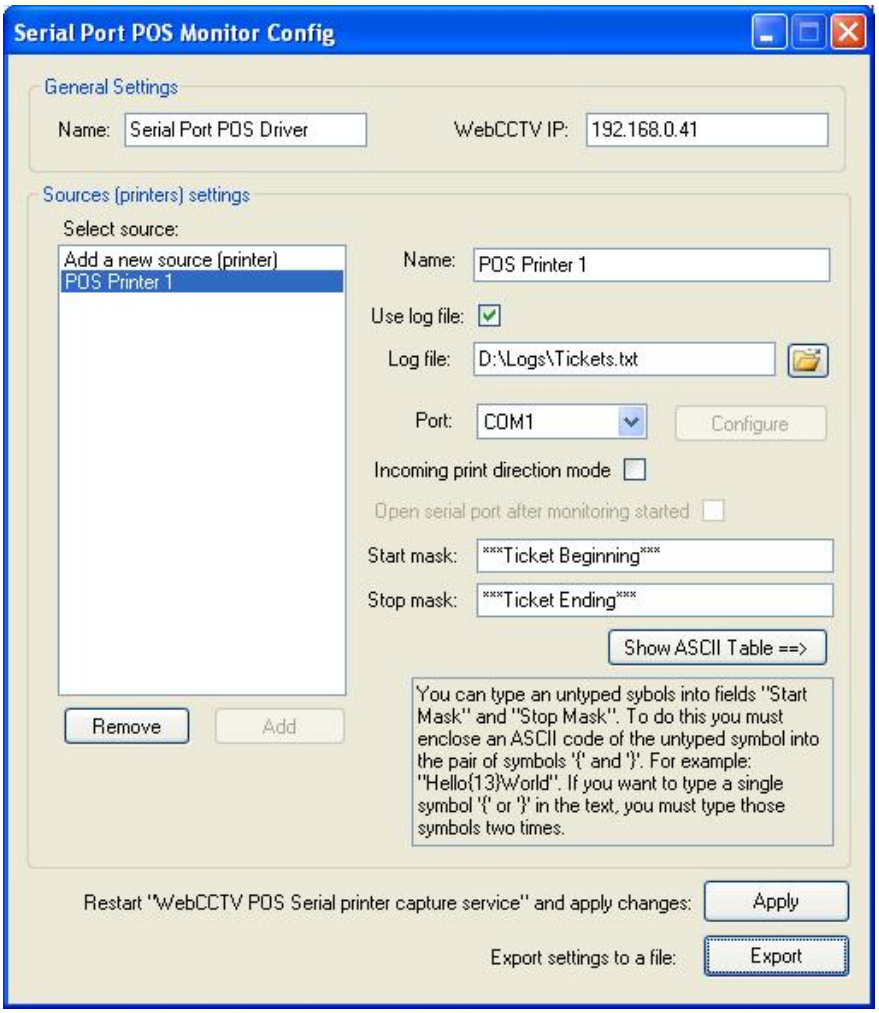
It is recommended to switch off logging when the configuration has been completed in order not to overload the hard disk with extra information. To do that, deselect the **Use log file** checkbox.

8. Check the **Incoming print direction mode** checkbox to enable monitoring of incoming data on the COM port.

You only have to check the box if you have incoming data. E.g. a hardware POS device connected to the COM port of the computer. If you have a POS device

(software based) installed on your computer, the direction mode will be outgoing.

9. Click the **Add** button.


Serial Port POS Monitor Config
General Settings
Name: Serial Port POS Driver
WebCCTV IP: 192.168.0.41
Sources (printers) settings
Select source:
Add a new source (printer)
POS Printer 1
Name: POS Printer 1
Use log file:
Log file: D:\Logs\Tickets.txt
Port: COM1
Configure
Incoming print direction mode
Open serial port after monitoring started
Start mask: ***Ticket Beginning***
Stop mask: ***Ticket Ending***
Show ASCII Table ==>
You can type an untyped sybols into fields "Start Mask" and "Stop Mask". To do this you must enclose an ASCII code of the untyped symbol into the pair of symbols '{' and '}'. For example: "Hello{13}World". If you want to type a single symbol '{' or '}' in the text, you must type those symbols two times.
Remove
Add
Restart "WebCCTV POS Serial printer capture service" and apply changes:
Apply
Export settings to a file:
Export

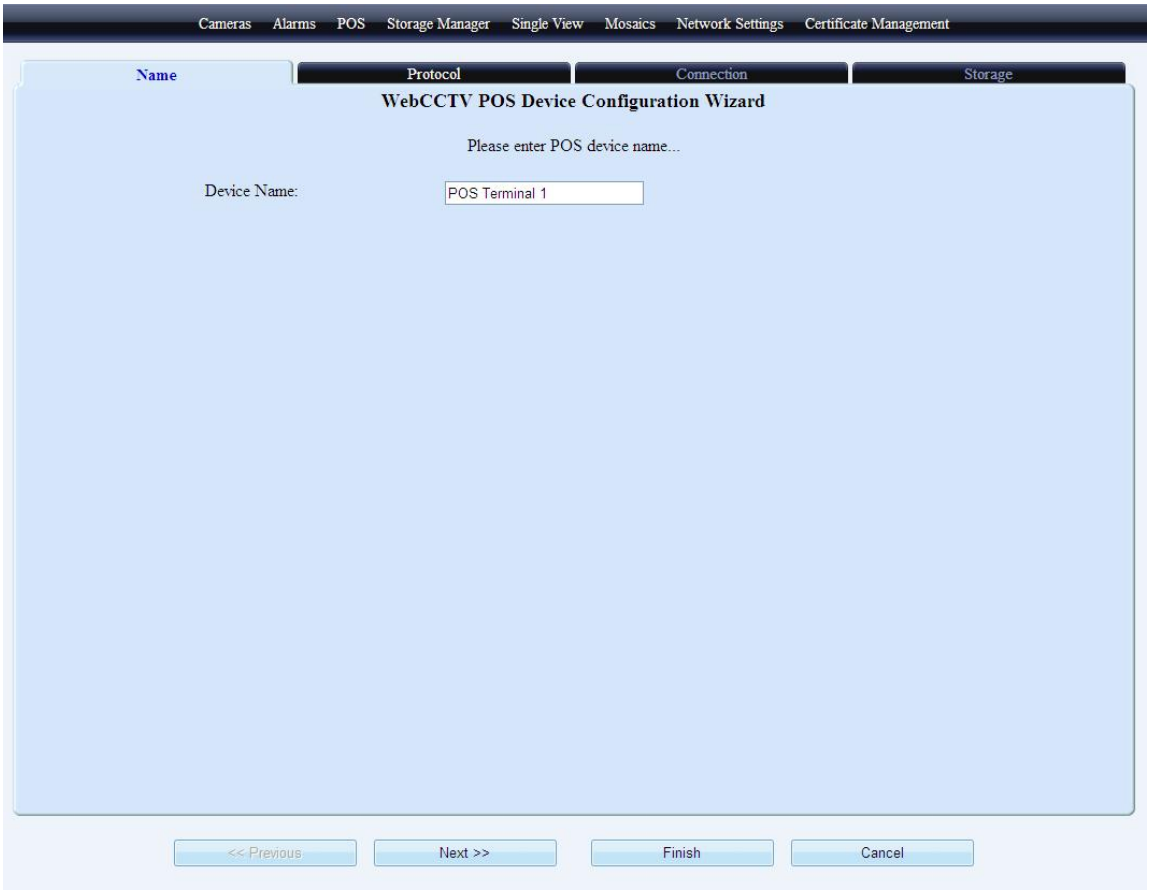
POS Monitor Configuration Screen

10. Click the **Apply** button to enable POS Monitor to monitor a newly added POS Printer.

You can export your Remote POS Monitor Configuration Application settings to a Registration Entries (.reg) file in order to be able to easily restore the configuration and add all the needed entries to the Windows registry later. To do so, click the **Export** button and save the file. In order to restore the configuration, double click the icon of the .reg file you created and confirm your intension to update the register information. The POS Printer (source) will be automatically added to the source list.

5.3.3.1.2 Name

In this tab, you can adjust the POS Device name. It's a part of the **POS Device Configuration Wizard.**



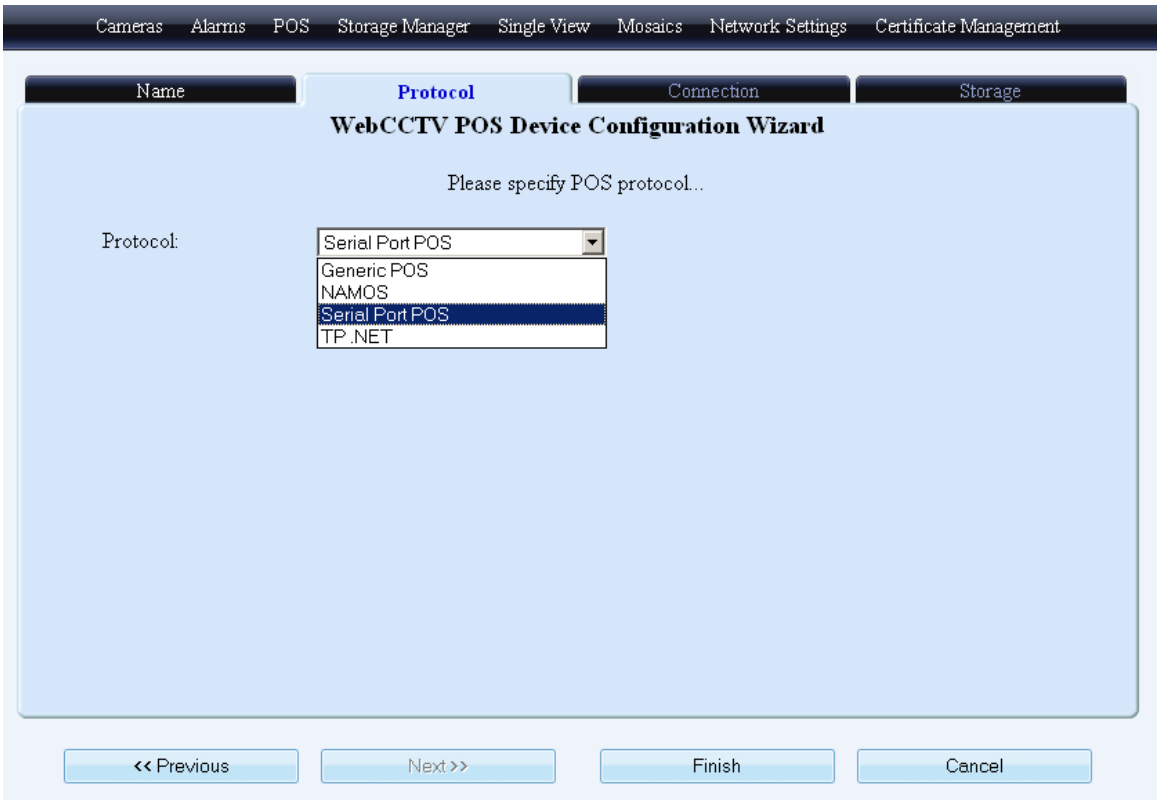
Name (Serial Port POS) Screen

Click **Next** to enter the next POS Device Configuration Wizard Screen.

5.3.3.1.3 Protocol

In this tab, the protocol has to be selected. It's a part of the **POS Device Configuration Wizard.**

Select **Serial Port POS** in the drop-down list.



Protocol (Serial Port POS) Screen

Click the **Finish** button.

Depending on the drivers you installed together with the Alarm Component, it's possible some values are not present in the drop-down list.

If you entered the POS Device Configuration Wizard by clicking the **Edit Device** link in the POS Screen, you can't change the protocol anymore, but you can only see which protocol has been selected.

5.3.3.1.4 Connection

This tab is not available for Serial Port POS Devices. You don't have to configure it.

5.3.3.1.5 Storage

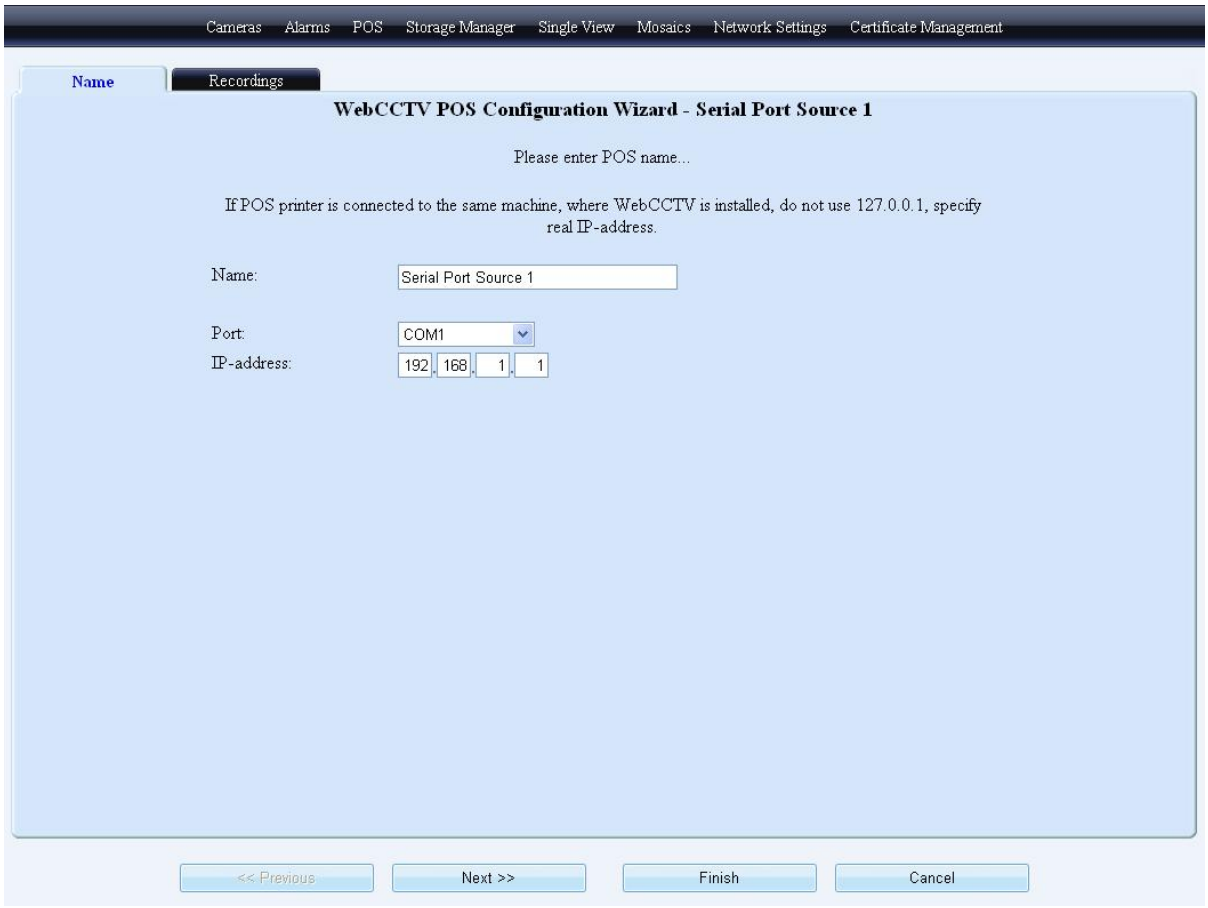
This tab is not available for Serial Port POS Devices. You don't have to configure it.

5.3.3.1.6 Name

This tab is a part of the **POS Configuration Wizard.** The following parameters have to be configured:

- **Name** – specify the name of the POS source.
- **Port** – select the COM port to which the POS source is connected.
- **IP address** – specify the IP address of the computer on which the POS source is connected.

If the WebCCTV server is installed on the same machine the POS printer is connected to, do not use the 127.0.0.1 IP address, but fill in the real IP-address. You can check the real IP address in the TCP/IP properties of your machine.



Name (Serial Port POS) Screen

Click **Next** to enter the next POS Configuration Wizard Screen.

5.3.3.1.7 Recordings

This tab is a part of the **POS Configuration Wizard**. In this tab you are able to do the following:

- Add or delete cameras to record when a ticket is generated.

Multiple recordings can be assigned to one source. This way, a ticket can be monitored from different cameras and angles.

- Set the recording time before and after a ticket is generated. This is also called the pre and post ticket recording interval.

A ticket movie is labelled recorded footage from a camera you attached to the ticket, i.e. when a ticket comes in, the specific period of time recorded from a specified camera is labelled and saved. Once the recording is complete, it appears as a ticket movie. If there aren't recordings (i.e. when there is no activity) for the period when the ticket is generated, you won't have a ticket movie. You can set a camera to record all the time via the Camera Configuration Wizard.

To add the camera to be recorded when a ticket is generated, follow the steps below:

1. Select the camera from the drop-down list.
2. Select the pre and post ticket label interval for each camera.
3. Click the **Add camera** button.

Recordings (Serial Port POS) Screen

To delete a camera, click **Delete**.

Click the **Finish** button.

5.3.3.2 Generic POS

The **Generic POS Device** makes it possible to generate transaction tickets without needing a POS Device. Generating tickets is done by using the SDK (Software Development Kit). For more information on how to use the SDK Kit, contact SDK@quadrox.be.

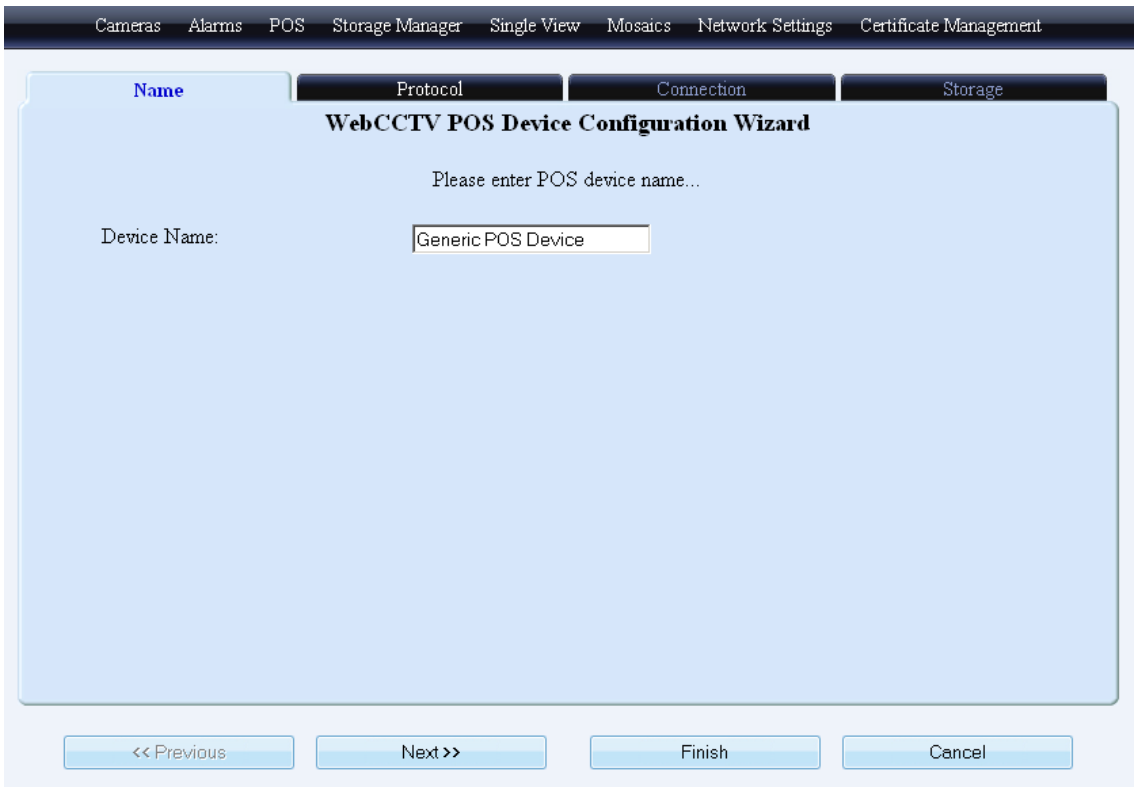
In order to add and configure your Generic POS device, click the **Edit device** or **Add POS Device** link/button in the POS screen. The **POS Device Configuration Wizard** consists of four tabs with easy to follow instructions.

In order to configure the sources, click the **Edit** link of the source in the POS screen which will lead you to the POS configuration Wizard. The **POS Configuration Wizard** consists of two tabs with easy to follow instructions.

The POS functionality is a part of the WebCCTV Alarm Component. You need to have the Alarm Component installed before you can use the POS functionality.

5.3.3.2.1 Name

In this tab, you can adjust the Generic POS device name. It's a part of the **POS Device Configuration Wizard.**



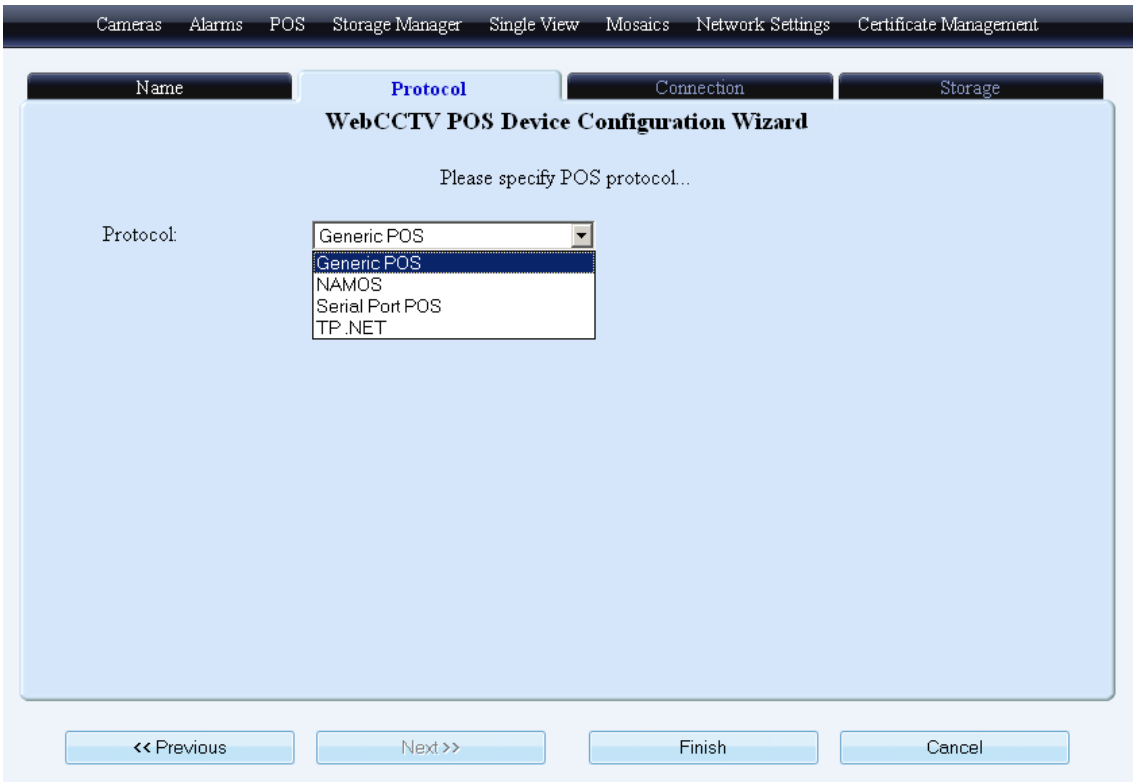
Name (Generic POS) Screen

Click **Next** to enter the next POS Device Configuration Wizard Screen.

5.3.3.2.2 Protocol

In this tab, the protocol has to be selected. It's a part of the **POS Device Configuration Wizard.**

Select **Generic POS** in the drop-down list.



Protocol (Generic POS) Screen

Click the **Finish** button.

Depending on the drivers you installed together with the Alarm Component, it's possible some options are not present in the drop-down list.

If you entered the POS Device Configuration Wizard by clicking the Edit Device link in the POS Screen, you can no longer change the protocol.

5.3.3.2.3 Connection

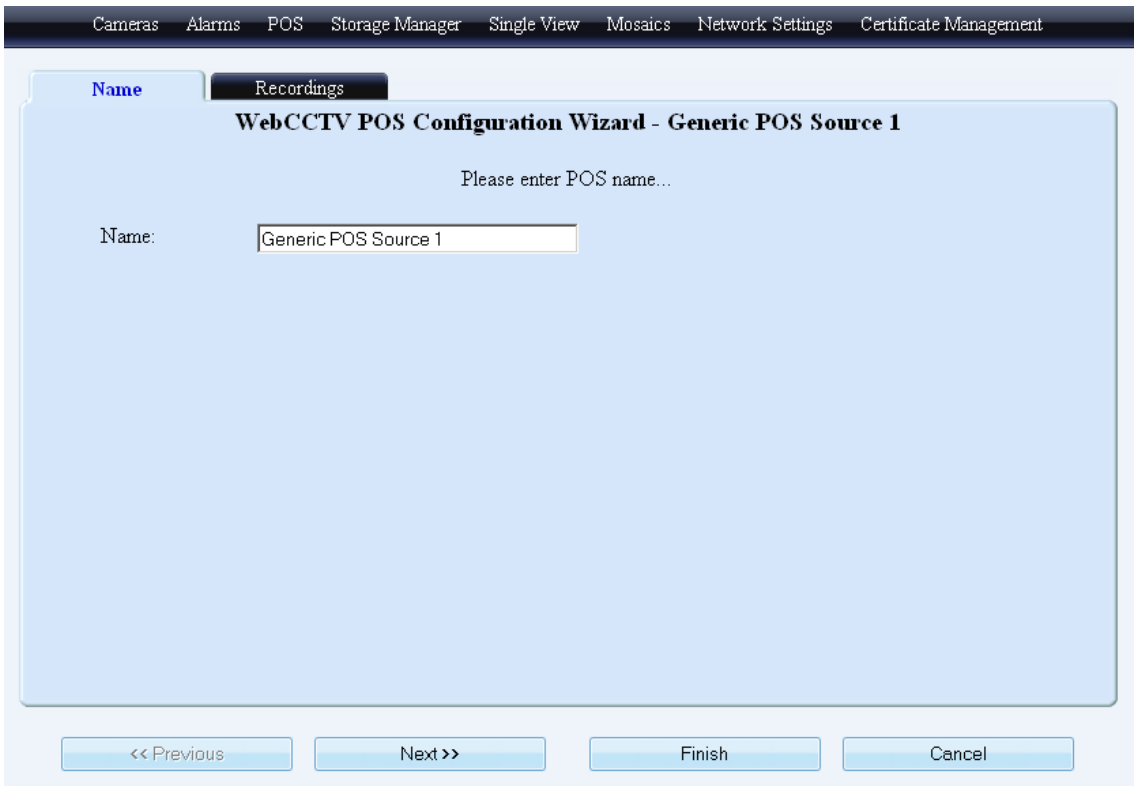
This tab is not available for Generic POS Devices. You don't have to configure it.

5.3.3.2.4 Storage

This tab is not available for Generic POS Devices. You don't have to configure it.

5.3.3.2.5 Name

In this tab, you can adjust the Generic POS source name. It's a part of the **POS Configuration Wizard.**



Name (Generic POS) Screen

Click **Next** to enter the next POS Configuration Wizard Screen.

5.3.3.2.6 Recordings

This tab is a part of the **POS Configuration Wizard**. In this tab you are able to do the following:

- Add or delete cameras to record when a ticket is generated.

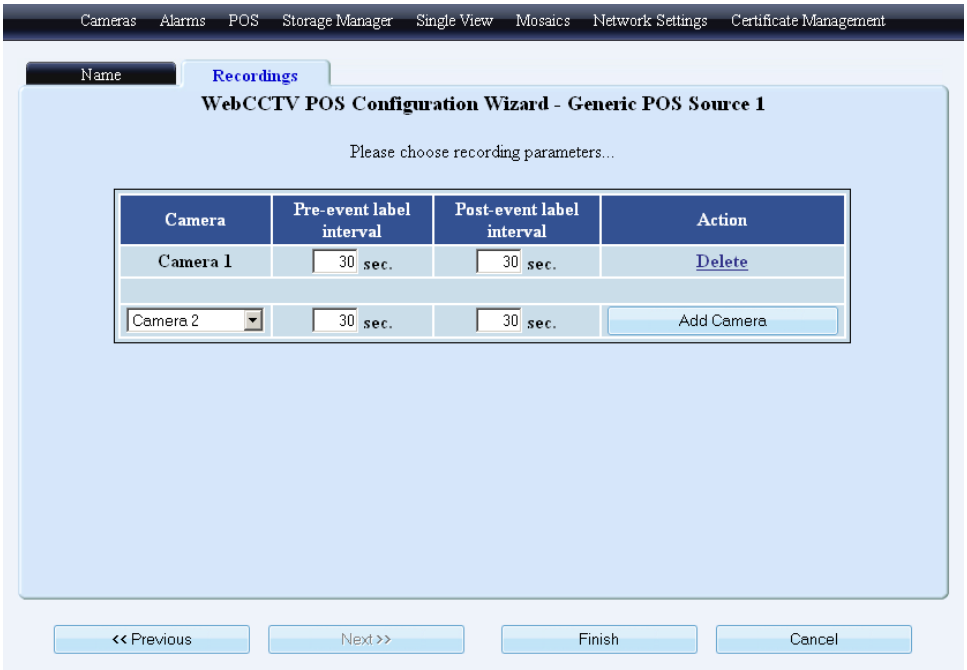
Multiple recordings can be assigned to one source. This way, a ticket can be monitored from different cameras and angles.

- Set the recording time before and after a ticket is generated. This is also called the pre and post ticket recording interval.

A ticket movie is labelled recorded footage from a camera you attached to the ticket, i.e. when a ticket comes in, the specific period of time recorded from a specified camera is labelled and saved. Once the recording is complete, it appears as a ticket movie. If there aren't recordings (i.e. when there is no activity) for the period when the ticket is generated, you won't have a ticket movie. You can set a camera to record all the time via the Camera Configuration Wizard.

To add the camera to be recorded when a ticket is generated, follow the steps below:

1. Select the camera from the drop-down list.
2. Select the pre and post ticket label interval for each camera.
3. Click the **Add camera** button.



Recordings (Generic POS) Screen

To delete a camera, click **Delete**.

Click the **Finish** button.

5.3.3.3 TP.Net

The TP.Net device has to be configured on both sides. This means at the TP.Net software side and at the WebCCTV side. We only discuss the WebCCTV side. For the TP.Net software side, consult the TP.Net documentation.

In order to add and configure your POS device, click the **Edit device** or **Add POS Device** link/button in the POS screen. The **POS Device Configuration Wizard** consists of four tabs with easy to follow instructions.

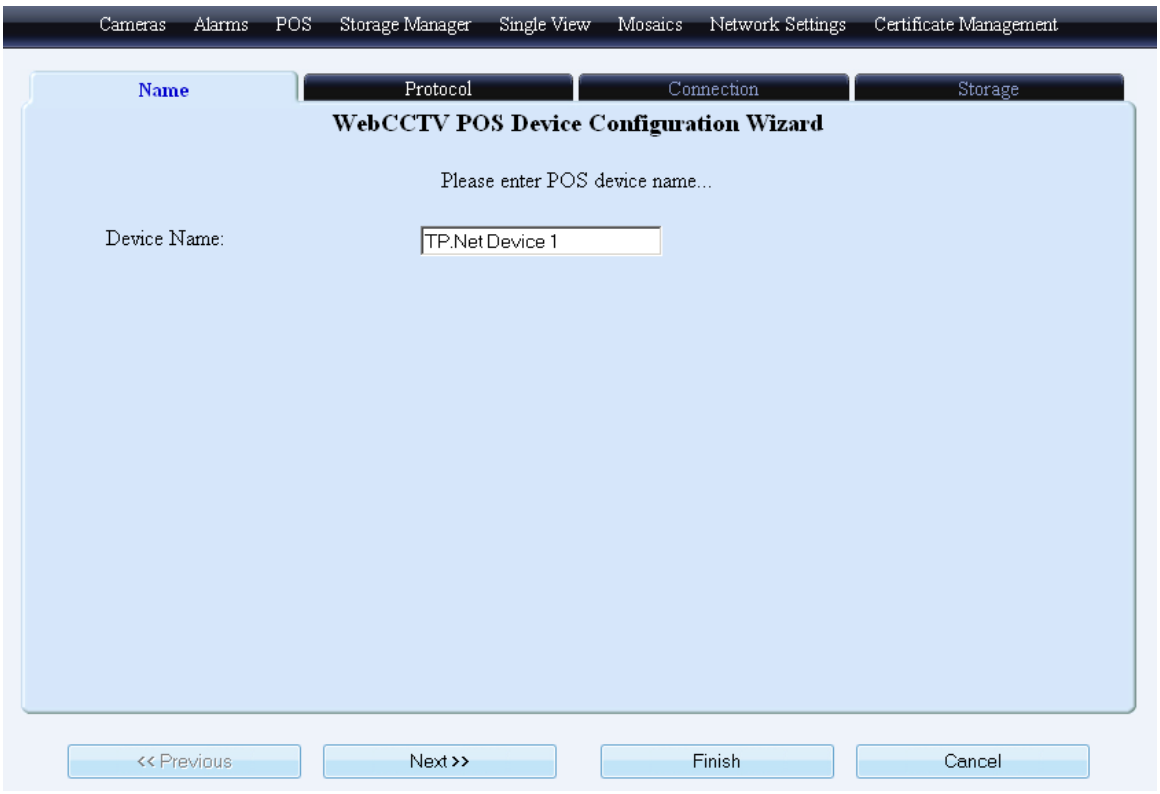
In order to configure the sources, click the **Edit** link of the source in the POS screen which will lead you to the POS configuration Wizard. The **POS Configuration Wizard** consists of two tabs with easy to follow instructions.

The POS functionality is a part of the WebCCTV Alarm Component. You need to have the Alarm Component installed before you can use the POS functionality.

You need to select the TP.Net driver in the custom menu when installing the Alarm Component. By default only the Serial Port POS and Generic POS driver is installed when installing the Alarm Component.

5.3.3.3.1 Name

In this tab, you can adjust the POS Device name. It's a part of the **POS Device Configuration Wizard.**



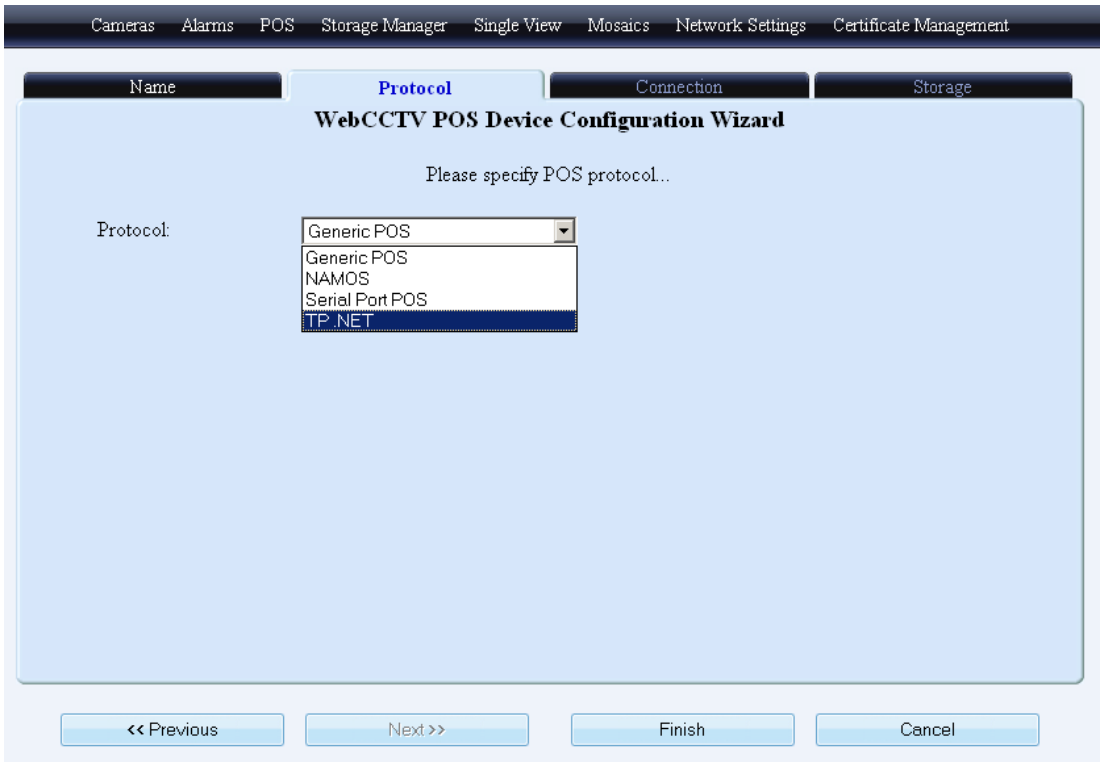
Name (TP.Net) Screen

Click **Next** to enter the next POS Device Configuration Wizard Screen.

5.3.3.3.2 Protocol

In this tab, the protocol has to be selected. It's a part of the **POS Device Configuration Wizard.**

Select **TP.NET** in the drop-down list.



Protocol (TP.Net) Screen

Click the **Finish** button. You will end up in the **Connection** tab of the POS Device Configuration Wizard.

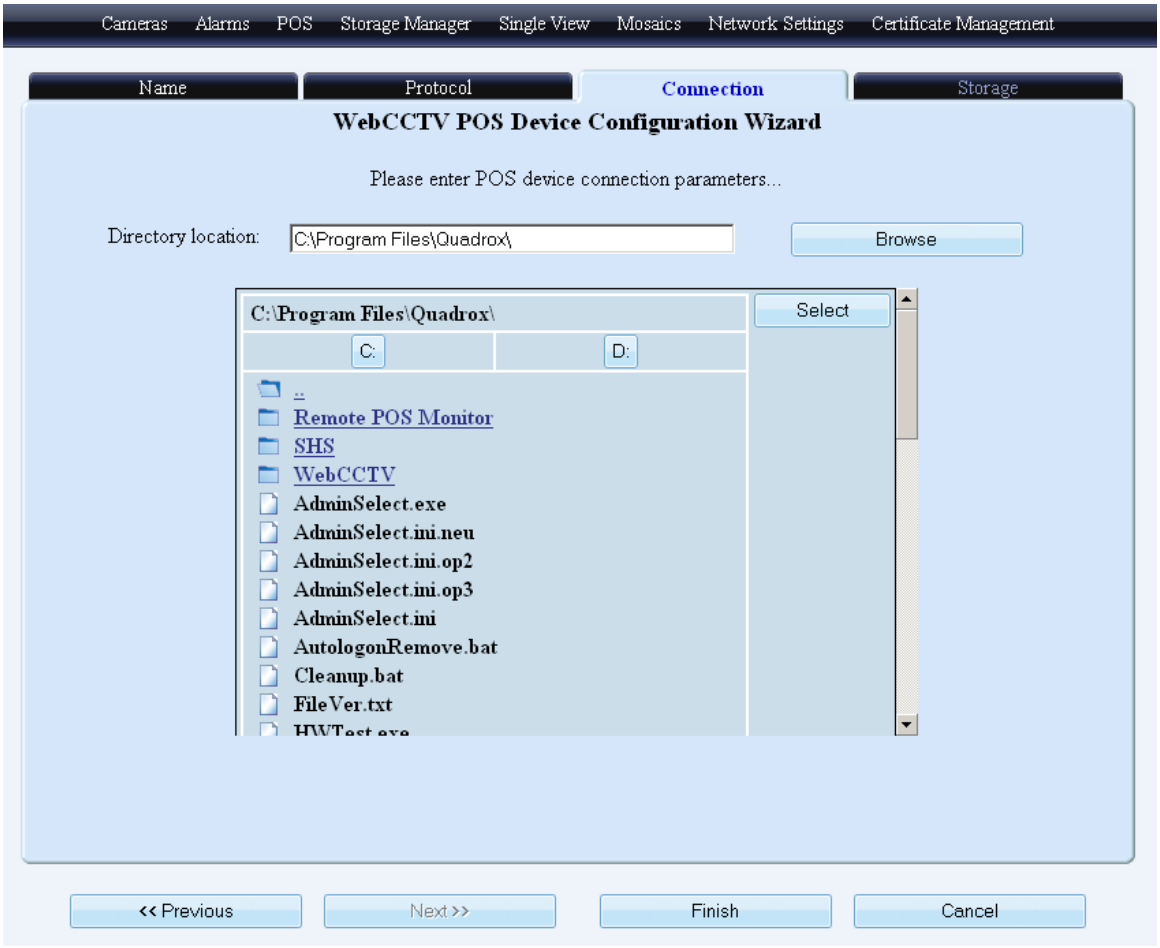
Depending on the drivers you installed together with the Alarm Component, it's possible some options are not present in the drop-down list.

If you entered the POS Device Configuration Wizard by clicking the **Edit Device** link in the POS Screen, you can no longer change the protocol.

5.3.3.3.3 Connection

In this tab, the connection has to be established. It's a part of the **POS Device Configuration Wizard.**

Select the directory where the PosLog compliant .xml files are saved by clicking the **Browse** button and the **Select** button.



Connection (TP.Net) Screen

Click the **Finish** button.

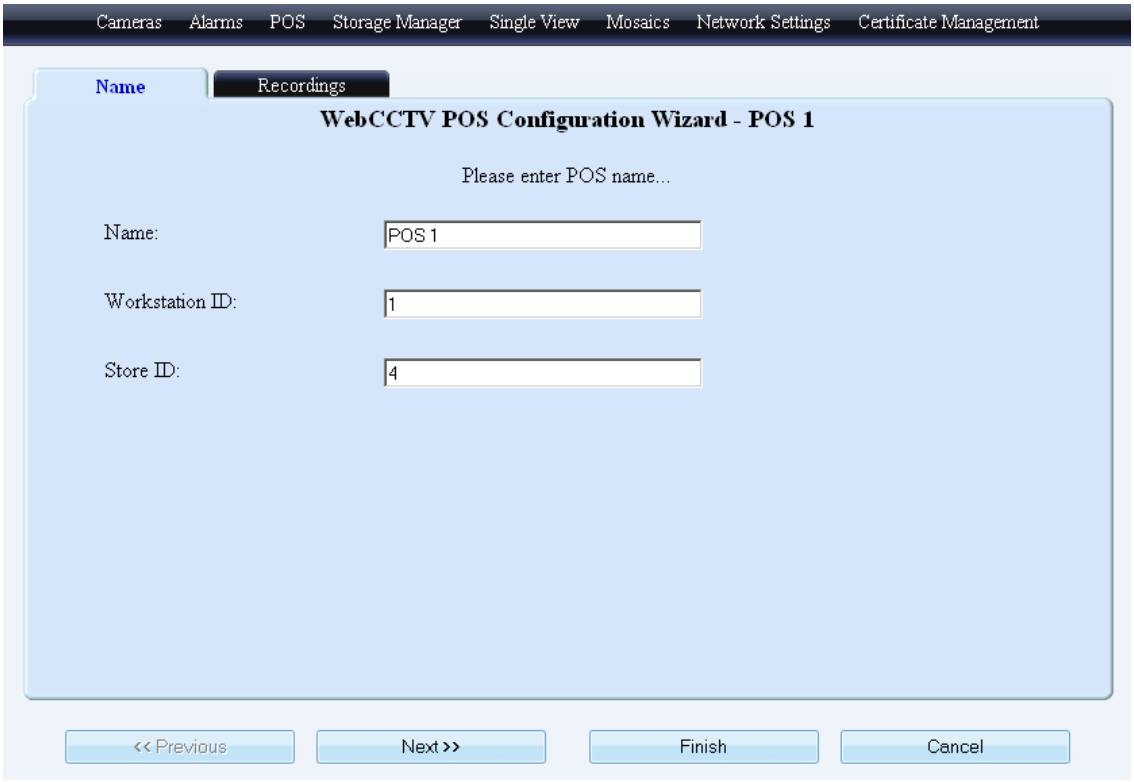
5.3.3.3.4 Storage

This tab is not available for TP.Net Devices. You don't have to configure it.

5.3.3.3.5 Name

This tab is a part of the **POS Configuration Wizard.** The following parameters have to be configured:

- **Name** – specify the name of the POS source.
- **Workstation ID** – specify the workstation ID.
- **Store ID** – specify the store ID.



Name (TP.Net) Screen

Click **Next** to enter the next POS Configuration Wizard Screen.

5.3.3.3.6 Recordings

This tab is a part of the **POS Configuration Wizard**. In this tab you are able to do the following:

- Add or delete cameras to record when a ticket is generated.

Multiple recordings can be assigned to one source. This way, a ticket can be monitored from different cameras and angles.

- Set the recording time before and after a ticket is generated. This is also called the pre and post ticket recording interval.

A ticket movie is labelled recorded footage from a camera you attached to the ticket, i.e. when a ticket comes in, the specific period of time recorded from a specified camera is labelled and saved. Once the recording is complete, it appears as a ticket movie. If there aren't recordings (i.e. when there is no activity) for the period when the ticket is generated, you won't have a ticket movie. You can set a camera to record all the time via the Camera Configuration Wizard.

To add the camera to be recorded when a ticket is generated, follow the steps below:

1. Select the camera from the drop-down list.
2. Select the pre and post ticket label interval for each camera.
3. Click the **Add camera** button.

Recordings (TP.Net) Screen

To delete a camera, click **Delete**.

Click the **Finish** button.

5.3.3.4 NAMOS

The NAMOS device has to be configured on both sides. This means on the NAMOS software side and at the WebCCTV side. We only discuss the WebCCTV side. For the NAMOS software side, consult the NAMOS documentation.

In order to add and configure your POS device, click the **Edit device** or **Add POS Device** link/button in the POS screen. The **POS Device Configuration Wizard** consists of four tabs with easy to follow instructions.

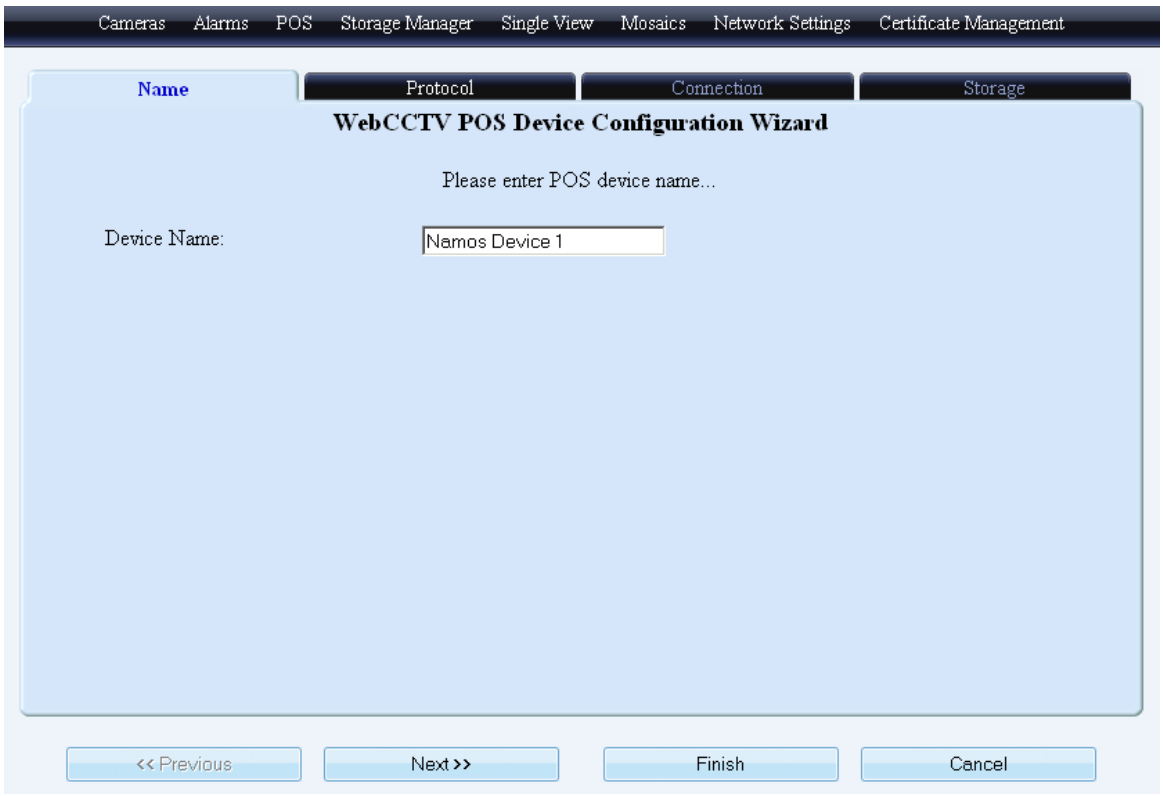
In order to configure the sources, click the **Edit** link of the source in the POS screen which will lead you to the POS configuration Wizard. The **POS Configuration Wizard** consists of two tabs with easy to follow instructions.

The POS functionality is a part of the WebCCTV Alarm Component. You need to have the Alarm Component installed before you can use the POS functionality.

You need to select the NAMOS driver in the custom menu when installing the Alarm Component. By default only the Serial Port POS and Generic POS driver is installed when installing the Alarm Component.

5.3.3.4.1 Name

In this tab, you can adjust the POS Device name. It's a part of the **POS Device Configuration Wizard.**



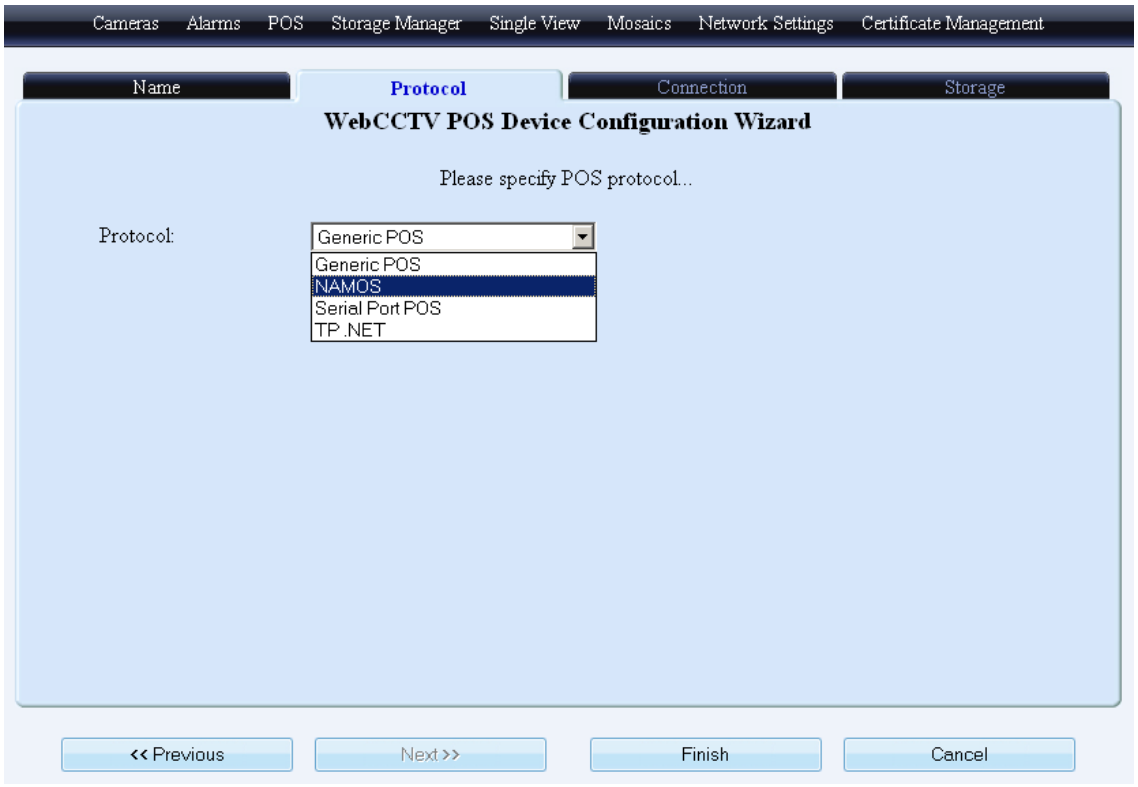
Name (NAMOS) Screen

Click **Next** to enter the next POS Device Configuration Wizard Screen.

5.3.3.4.2 Protocol

In this tab, the protocol has to be selected. It's a part of the **POS Device Configuration Wizard.**

Select **NAMOS** in the drop-down list.



Protocol (NAMOS) Screen

Click the **Finish** button.

Depending on the drivers you installed together with the Alarm Component, it's possible some options are not present in the drop-down list.

If you entered the POS Device Configuration Wizard by clicking the Edit Device link in the POS Screen, you can no longer change the protocol.

5.3.3.4.3 Connection

This tab is not available for NAMOS Devices. You don't have to configure it.

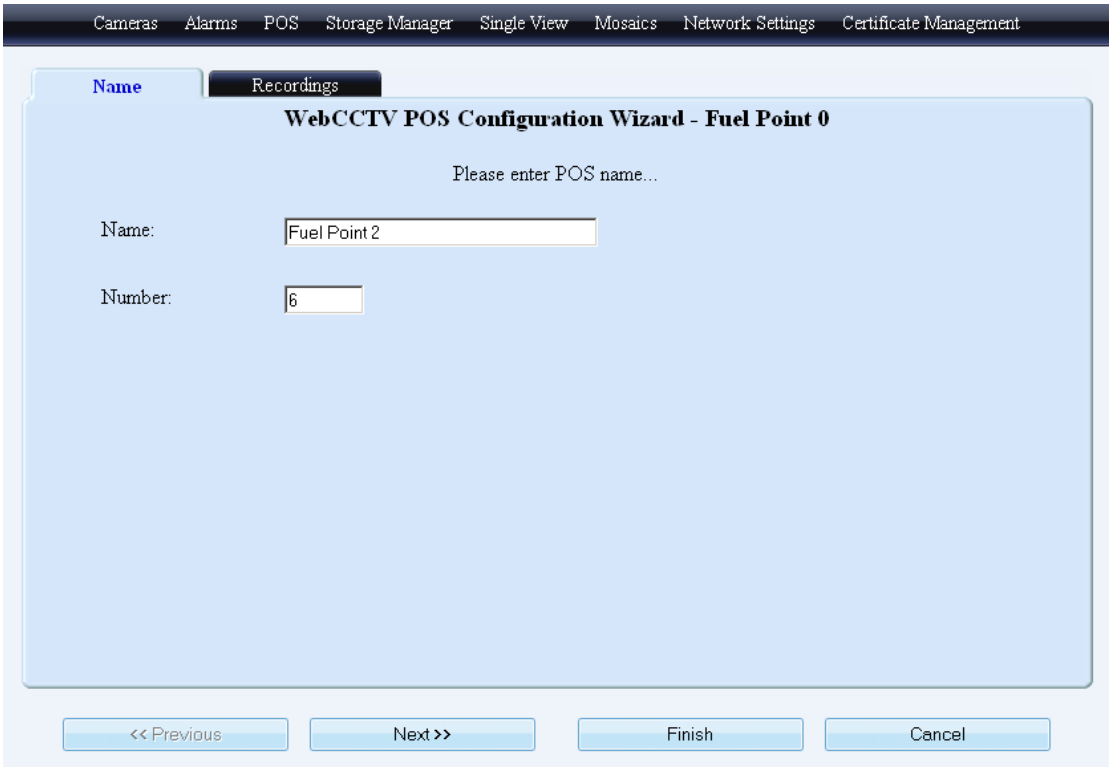
5.3.3.4.4 Storage

This tab is not available for NAMOS Devices. You don't have to configure it.

5.3.3.4.5 Name

This tab is a part of the **POS Configuration Wizard.** The following parameters have to be configured:

- **Name** – specify the name of the POS source.
- **Number** – specify the number.



Name (NAMOS) Screen

Click **Next** to enter the next POS Configuration Wizard Screen.

5.3.3.4.6 Recordings

This tab is a part of the **POS Configuration Wizard**. In this tab you are able to do the following:

- Add or delete cameras to record when a ticket is generated.

Multiple recordings can be assigned to one source. This way, a ticket can be monitored from different cameras and angles.

- Set the recording time before and after a ticket is generated. This is also called the pre and post ticket recording interval.

A ticket movie is labelled recorded footage from a camera you attached to the ticket, i.e. when a ticket comes in, the specific period of time recorded from a specified camera is labelled and saved. Once the recording is complete, it appears as a ticket movie. If there aren't recordings (i.e. when there is no activity) for the period when the ticket is generated, you won't have a ticket movie. You can set a camera to record all the time via the Camera Configuration Wizard.

To add the camera to be recorded when a ticket is generated, follow the steps below:

1. Select the camera from the drop-down list.
2. Select the pre and post ticket label interval for each camera.
3. Click the **Add camera** button.

Recordings (NAMOS) Screen

To delete a camera, click **Delete**.

Click the **Finish** button.

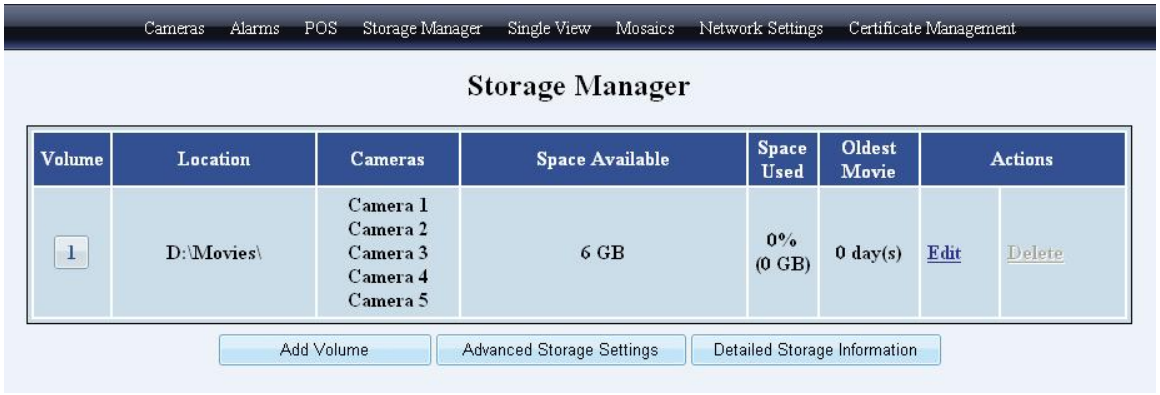
5.3.4 Storage Manager

This chapter describes the **Storage Manager** menu. This menu gives you the ability to manage the volumes the movies are recorded to. It provides detailed information about every volume and the recordings stored on it. It allows adding or deleting cameras from a certain volume, disabling volumes etc.

The following topics are discussed:

- Adding, configuring & deleting a volume
- Advanced Storage Settings
- Detailed Storage Information

You must be very careful while performing any manipulations of volumes as this may erase all the footage from the cameras assigned to the volumes being manipulated.



Storage Manager Screen

5.3.4.1 Adding, configuring & deleting a Volume

Since WebCCTV supports multivolume recording, several volumes can be added to one server. To enter the Volume Configuration Wizard, click the **Edit** or **Add Volume** link/button in the Storage Manager screen. The **Volume Configuration Wizard** consists of three tabs with easy to follow instructions.

The following **Volume Configuration Wizards** tabs are described:

- Location
- Cameras
- Storage Parameters

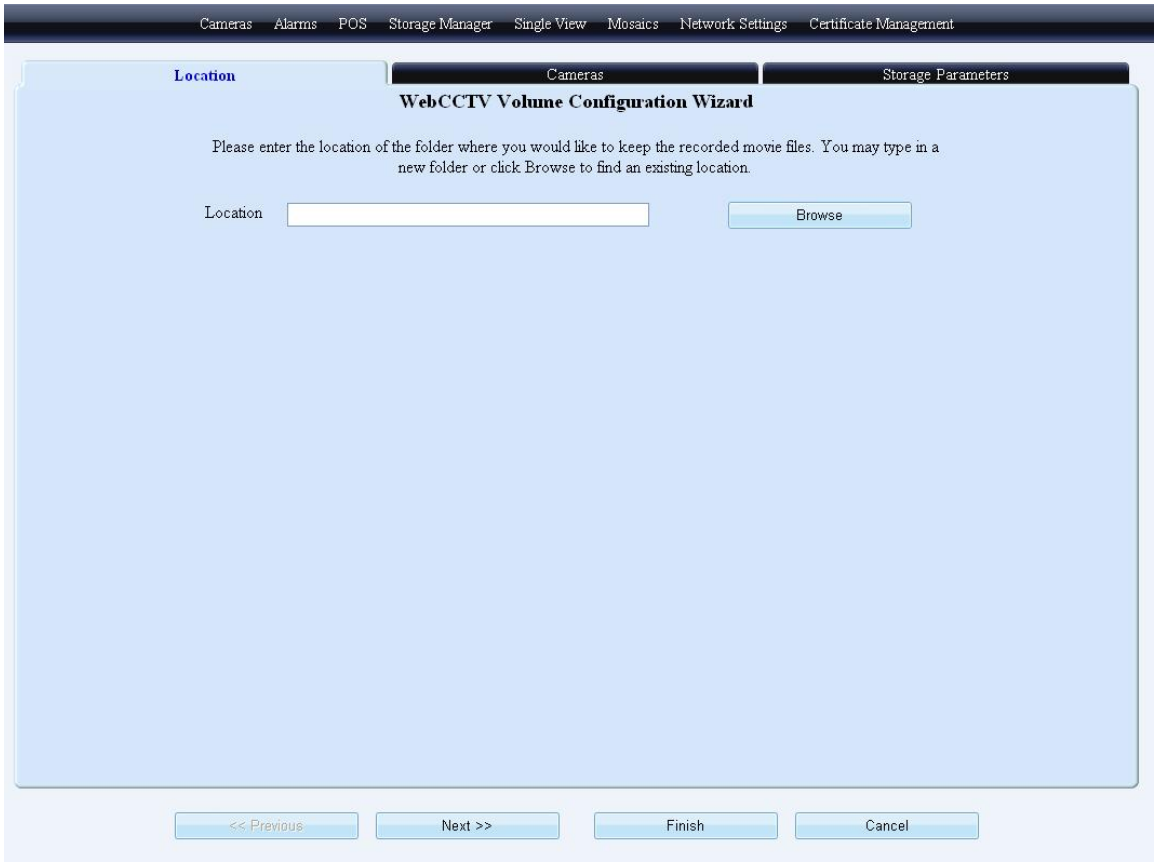
You cannot delete all volumes added to your system. In case only one volume is left, the **Delete** link will be disabled. Furthermore you can't delete a volume if there are cameras assigned. First reassign all cameras to another volume.

To delete a volume, click the **Delete** link. Click **OK** on the screen that pops up.

5.3.4.1.1 Location

This tab allows you to select the location of the folder wherein you want to store your recordings.

Only one volume per partition can be created. For example, if you have your footage being recorded to **D:\Movies** folder, you cannot specify **D:\New_Movies** as a new volume. The partition letter has to be unique for each volume.

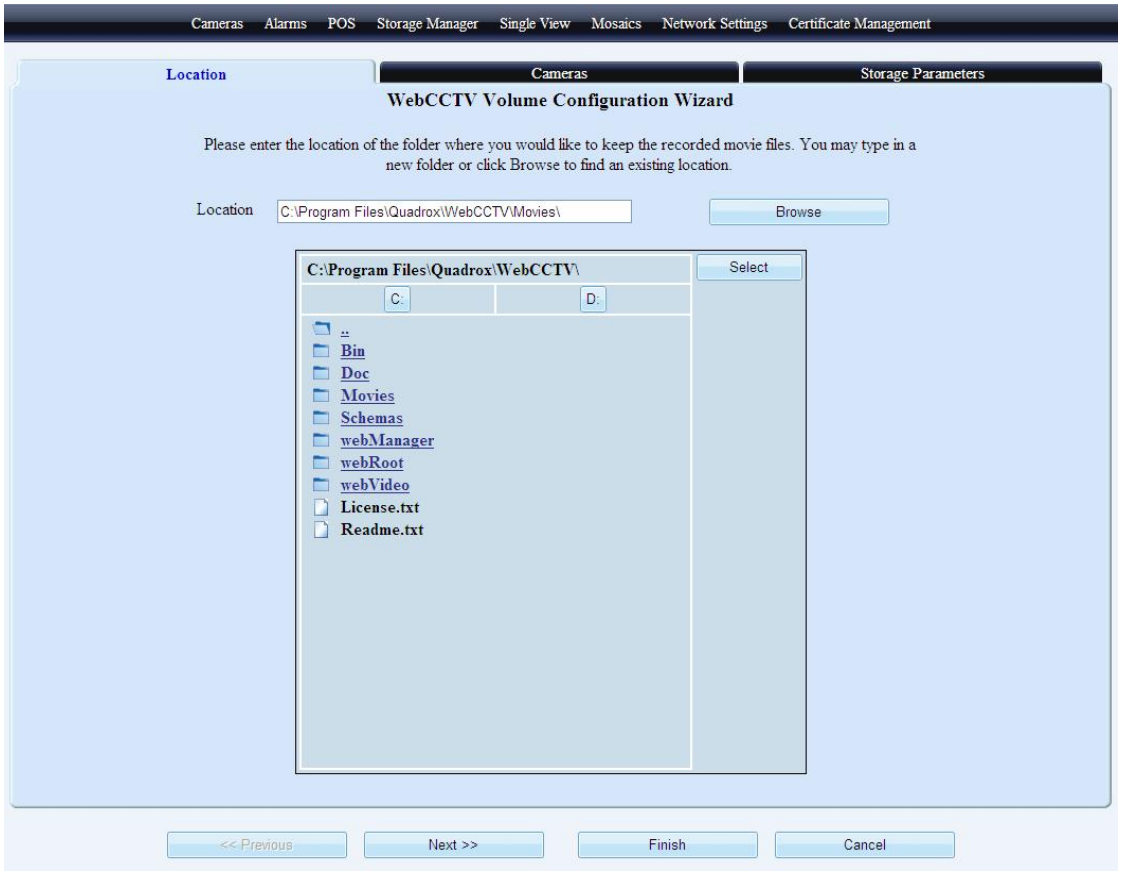


Location Screen

Enter the path and the name of the folder in the **Location** field that will be used to store recordings.

If you entered the Volume Configuration Wizard by clicking the Edit link, you will not be able to change the location. You can choose the location only when adding a new volume.

Click the **Browse** button to open a table. The following screen will appear:



Location (Browse) Screen

Browse the table and choose the folder you would like to use for storing recordings. Click the **Select** button to confirm your selection.

In case you enter the path and name of a folder which doesn't exist, it will be created automatically.

Click **Next** to enter the next Volume Configuration Wizard Screen.

5.3.4.1.2 Cameras

This tab allows you to assign cameras to a volume.

Cameras Screen

By default only one volume is created during installation and thus all the cameras added will be automatically assigned to this volume. If you add a volume after you added all the cameras to your system, you will have to reassign those cameras from the "old" volume to a newly created one which will erase all the recordings from these cameras on your previous volume. Therefore it is recommended to manage your volumes before you add cameras to your system.

To add a camera to a volume, follow the steps below:

1. Select a camera from the drop-down list.
2. Click the **Add Camera** button.

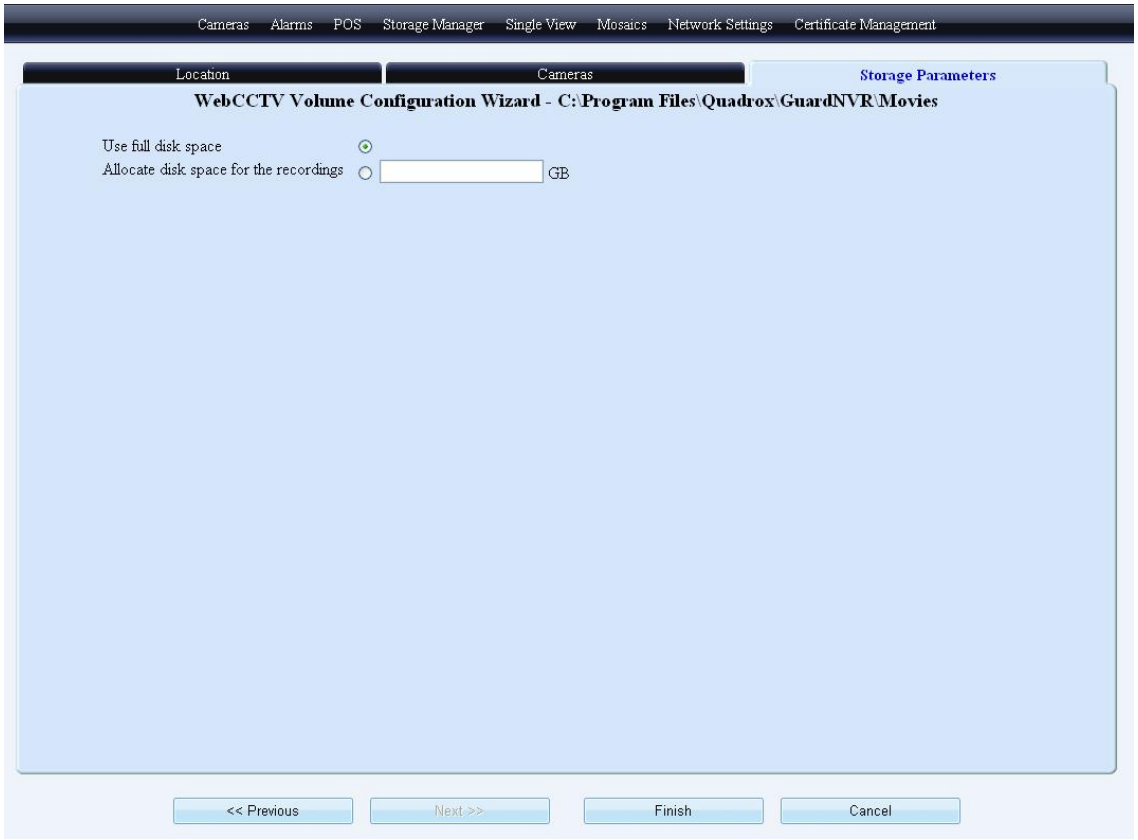
When finished adding cameras to the volume, click **Next** to enter the next Volume Configuration Wizard Screen.

5.3.4.1.3 Storage Parameters

This tab gives you the ability to manage the disk space used by the recordings stored on the volume. Depending on whether you are adding or editing the volume, this tab will differ slightly.

When **adding** a volume, following parameters are present:

- **Use full disk space** – this option allows the recordings to use all space available on the volume.
- **Allocate disk space for the recordings** – this option allows limiting the space used by recordings. In order to limit the space, select the corresponding radio button and enter an integer number (in gigabytes) that will be allocated for recordings.



Storage Parameters (Add) Screen

Click the **Finish** button.

When editing a volume, the following parameters are present:

- **Available disk space for recordings** – shows the amount of disk space on the volume that is assigned for recordings.
- **Space used by recordings** – shows the amount of space on the volume that is currently used by recordings.
- **Free space left** – shows the amount of space on the volume that is left for recordings.
- **Estimated disk space usage** – shows the estimated amount of space that will be used for recordings for one day.

- **Estimated time of recording** – shows the estimated amount of days that can be recorded.
- **Oldest movie** – shows how old the oldest movie on the volume is.
- **Clean up** – shows when the backup functionality cleaned up the volume for the last time in order to make space for recordings. The oldest movies are deleted first when the backup functionality starts.
- **Use full disk space** – this option allows the recordings to use all space available on the volume.
- **Allocate disk space for the recordings** – this option allows limiting the space used by recordings. In order to limit the space, select the corresponding radio button and enter an integer number (in gigabytes) that will be allocated for recordings.

Cameras
Alarms
POS
Storage Manager
Single View
Mosaics
Network Settings
Certificate Management
Location
Cameras
Storage Parameters
WebCCTV Volume Configuration Wizard - C:\Program Files\Quadrox\WebCCTV\Movies\
Available disk space for recordings: 6 GB
Space used by recordings: 0,3 GB
Free space left: 5,7 GB (95%)
With your current recordings configuration, you will use an estimate 23,3 GB per day on this volume.
With the current limitations that you have set, you can record for an estimated 0,2 day(s).
The oldest movie on this volume is 0 day(s) old.
The last recordings cleanup was at N/A
Use full disk space
Allocate disk space for the recordings
6
GB
<< Previous
Next >>
Finish
Cancel

Storage Parameters (Edit) Screen

Click the **Finish** button**.**

5.3.4.2 Advanced Storage Settings

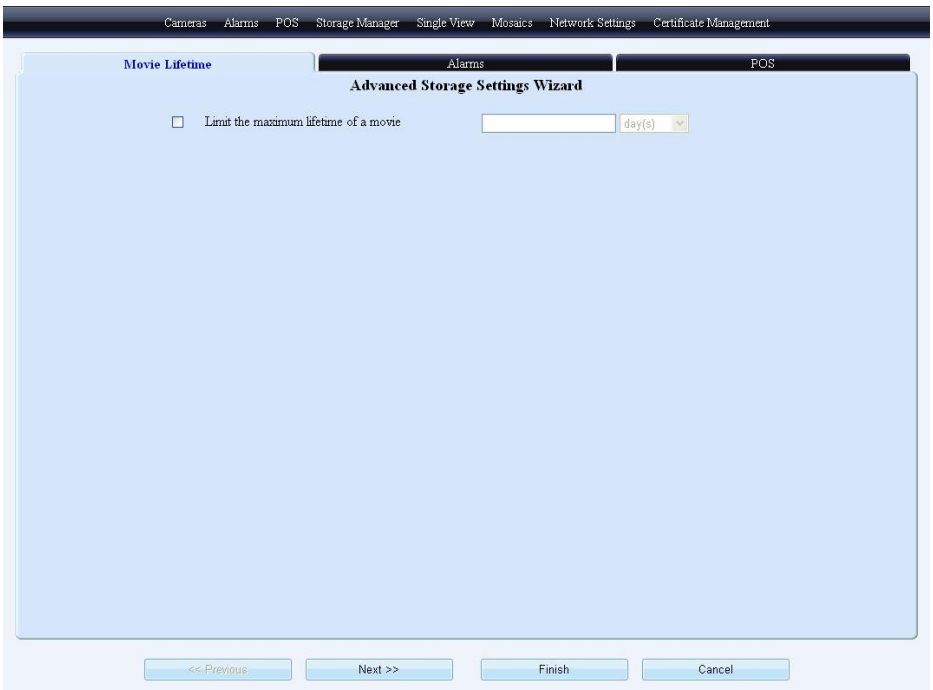
Click the **Advanced Storage Settings** button in the Storage Manager screen to open the Advanced Storage Settings Wizard. This menu allows for the configuration of the movie lifetime parameters for all types of movies.

The following **Advanced Storage Settings Wizards** tabs are described:

- Movie Lifetime
- Alarms
- POS

5.3.4.2.1 Movie Lifetime

This tab allows you to configure the **Maximum lifetime of a movie.** It is a value set in hours, days or months which determines the amount of time the recorded movies will be kept on the hard disk.



Movie Lifetime Screen

In order to set a movies lifetime limitation, follow the steps below:

1. Check the **Limit the maximum lifetime of a movie** checkbox.
2. Select the unit of time from the drop-down list (default unit is day(s)).
3. Enter an integer number indicating the period of time the movies will be kept (minimal value is 1).

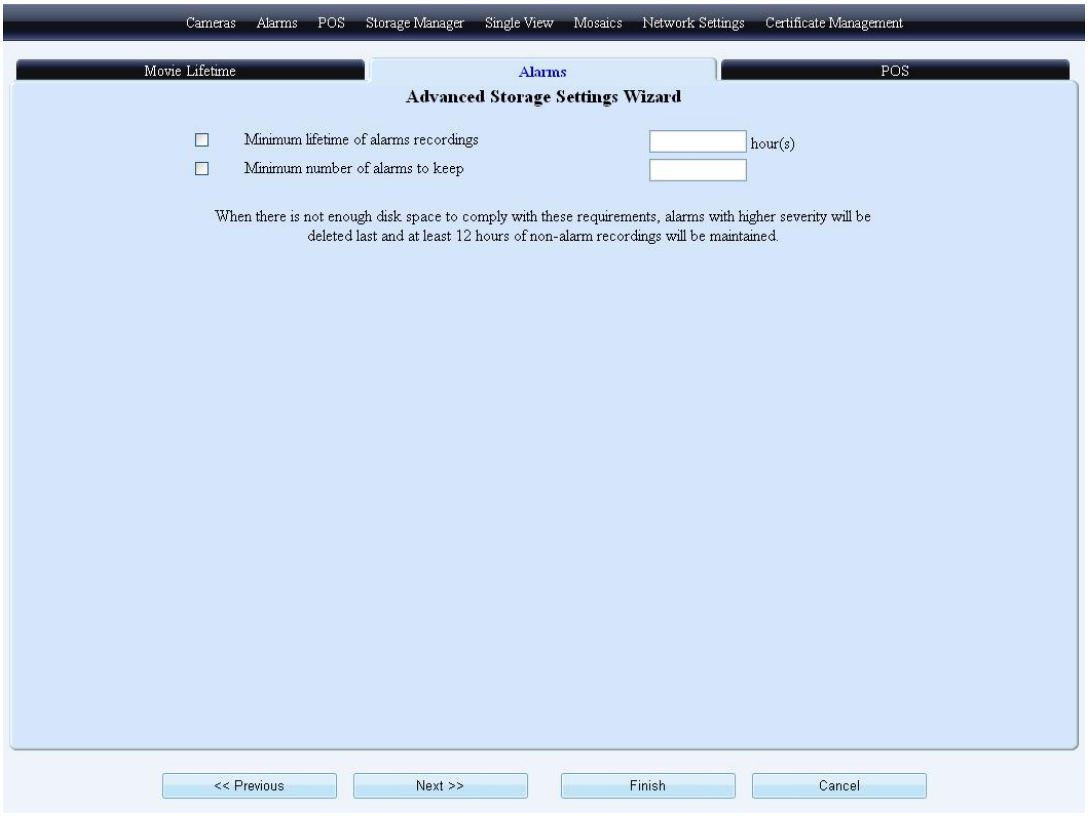
Click **Next** to enter the next Advanced Storage Settings Wizard Screen.

5.3.4.2.2 Alarms

This tab allows you to configure two parameters**:**

This tab will not be available unless the Alarm Component is installed.

- **Minimum lifetime of alarm recordings** – integer value set in hours and determines the amount of time the alarm movies will be kept on the hard disk. Check the checkbox if you want to activate this parameter.
- **Minimum number of alarms to keep** – integer value indicating the minimum number of alarms to keep. Check the checkbox if you want to activate this parameter.



Alarms Screen

When there is not enough disk space to comply with the requirements, alarms with higher priority will be deleted last and at least 12 hours of non-alarm recordings will be maintained.

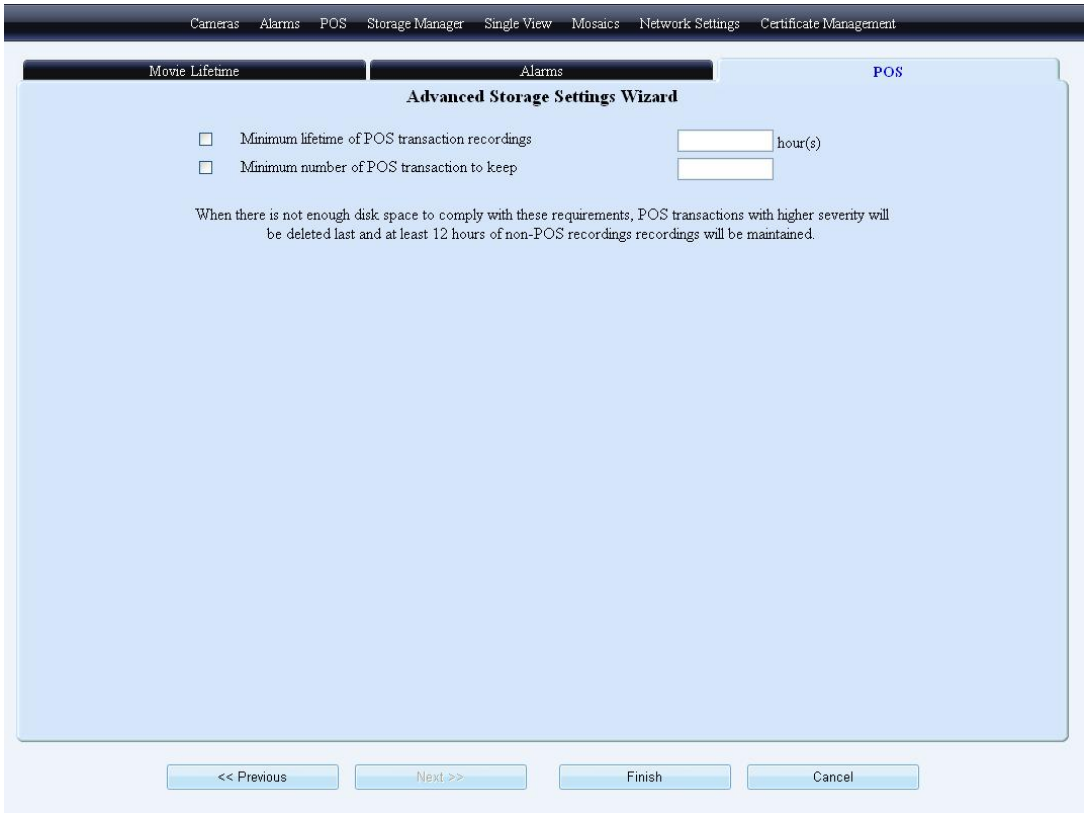
Click **Next** to enter next Advanced Storage Settings Screen.

5.3.4.2.3 POS

This tab allows you to configure two parameters**:**

This tab will not be available unless you have POS installed together with the Alarm Component.

- **Minimum lifetime of POS transaction recordings** – integer value set in hours and determines the amount of time the POS transaction movies will be kept on the hard disk. Check the checkbox if you want to activate this parameter.
- **Minimum number of POS transaction to keep** – integer value indicating the minimum number of POS transactions to keep. Check the checkbox if you want to activate this parameter.



POS Screen

When there is not enough disk space to comply with the requirements, POS transactions with higher severity will be deleted last and at least 12 hours of non-POS recordings will be maintained.

Click the **Finish** button.

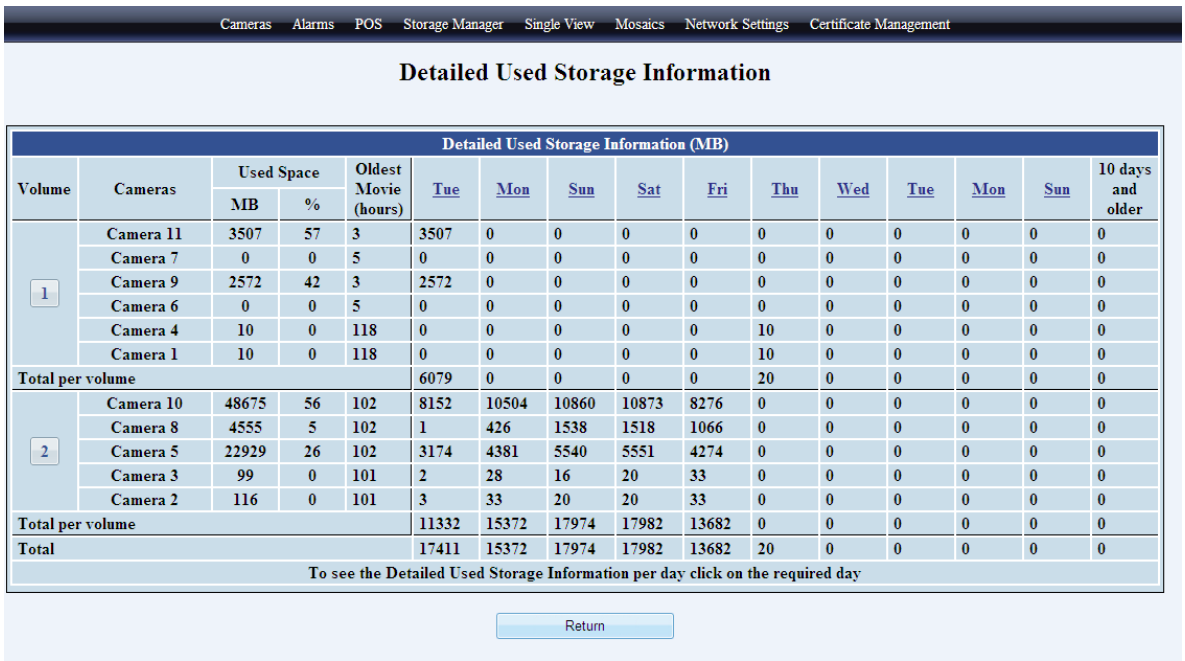
5.3.4.3 Detailed Storage Information

This menu gives you the detailed information about the space used by recordings from each camera on each volume.

The parameters shown here are measured in Megabytes.

The following info is available on a per camera basis in the **Detailed Used Storage Information** table:

- **Used space and % of total** – amount of disk space currently used by the recorded video footage from the particular camera in MB as well as the percentage used of the total available space.
- **Oldest movie (hours)** – age of oldest recorded video footage that belongs to this particular camera.
- **Days** columns – total size of recorded video footage from the particular camera for a particular day.
- **Total per volume** – storage space consumed by all cameras assigned to a particular volume for a particular day.
- **Total** – storage space consumed by all cameras for a particular day.


Cameras Alarms POS Storage Manager Single View Mosaics Network Settings Certificate Management
Detailed Used Storage Information
Detailed Used Storage Information (MB)
Volume Cameras Used Space MB % Oldest Movie (hours) Tue Mon Sun Sat Fri Thu Wed Tue Mon Sun 10 days and older
1 Camera 11 3507 57 3 3507 0 0 0 0 0 0 0 0 0 0
Camera 7 0 0 5 0 0 0 0 0 0 0 0 0 0 0
Camera 9 2572 42 3 2572 0 0 0 0 0 0 0 0 0 0
Camera 6 0 0 5 0 0 0 0 0 0 0 0 0 0 0
Camera 4 10 0 118 0 0 0 0 0 10 0 0 0 0 0
Camera 1 10 0 118 0 0 0 0 0 10 0 0 0 0 0
Total per volume 6079 0 0 0 0 20 0 0 0 0 0
2 Camera 10 48675 56 102 8152 10504 10860 10873 8276 0 0 0 0 0 0
Camera 8 4555 5 102 1 426 1538 1518 1066 0 0 0 0 0 0
Camera 5 22929 26 102 3174 4381 5540 5551 4274 0 0 0 0 0 0
Camera 3 99 0 101 2 28 16 20 33 0 0 0 0 0 0
Camera 2 116 0 101 3 33 20 20 33 0 0 0 0 0 0
Total per volume 11332 15372 17974 17982 13682 0 0 0 0 0 0
Total 17411 15372 17974 17982 13682 20 0 0 0 0 0
To see the Detailed Used Storage Information per day click on the required day
Return

Detailed Used Storage Information Screen

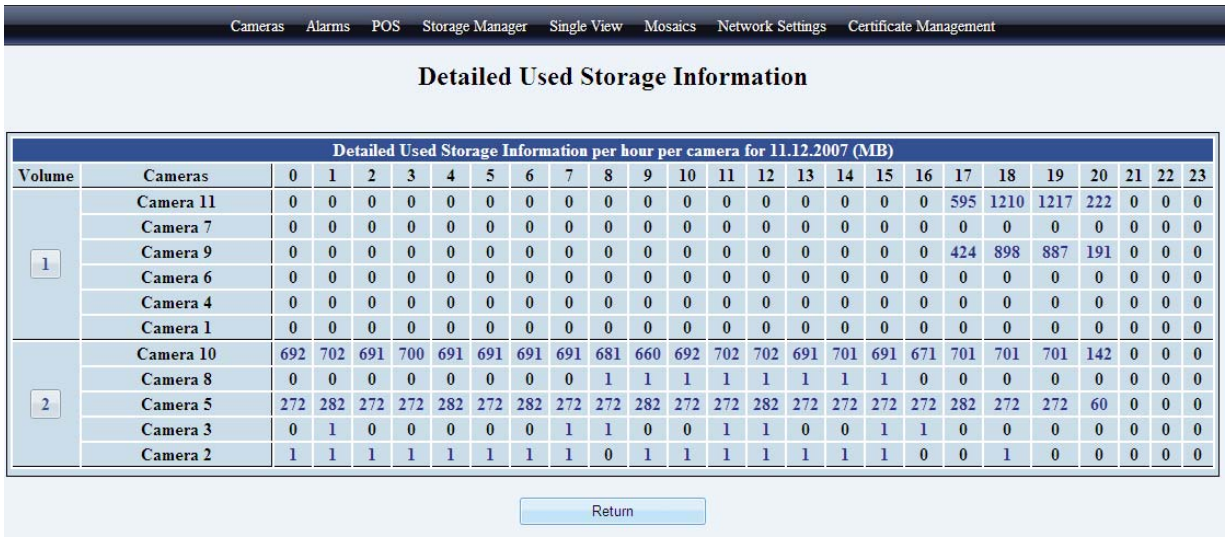
12.5% of the total space amount is reserved by the Operating System for the Master File Table (MFT). If free space becomes less then 12.5%, MFT begins to fragment. This process makes the Operating System slow. Therefore the maximum disk space that might be occupied by recordings is 87.5% of total disk space.

To return to the Storage Manager Screen, click **Return**.

The headers of each column in the table represent a day and are clickable. When clicking on the link, the **Detailed Used Storage Information per Day** table is shown.

There are 10 days for which more precise hour-by-hour information is available by clicking on the applicable days link. All the rest of the days are shown as a combined value in the "Older" column. The present's day data is displayed in the left column.

You can request the playback of a certain hour from a certain camera by clicking in the corresponding cell.


Cameras Alarms POS Storage Manager Single View Mosaics Network Settings Certificate Management
Detailed Used Storage Information
Detailed Used Storage Information per hour per camera for 11.12.2007 (MB)
Return

Volume	Cameras	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	Camera 11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	595	1210	1217	222	0	0	0
	Camera 7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Camera 9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	424	898	887	191	0	0	0
	Camera 6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Camera 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Camera 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Camera 10	692	702	691	700	691	691	691	691	681	660	692	702	702	691	701	691	671	701	701	701	142	0	0	0
	Camera 8	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
	Camera 5	272	282	272	272	282	272	282	272	272	282	272	272	282	272	272	272	272	282	272	272	60	0	0	0
	Camera 3	0	1	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0
	Camera 2	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	0	0	0	0	0

Detailed Used Storage Information (per Day) Screen

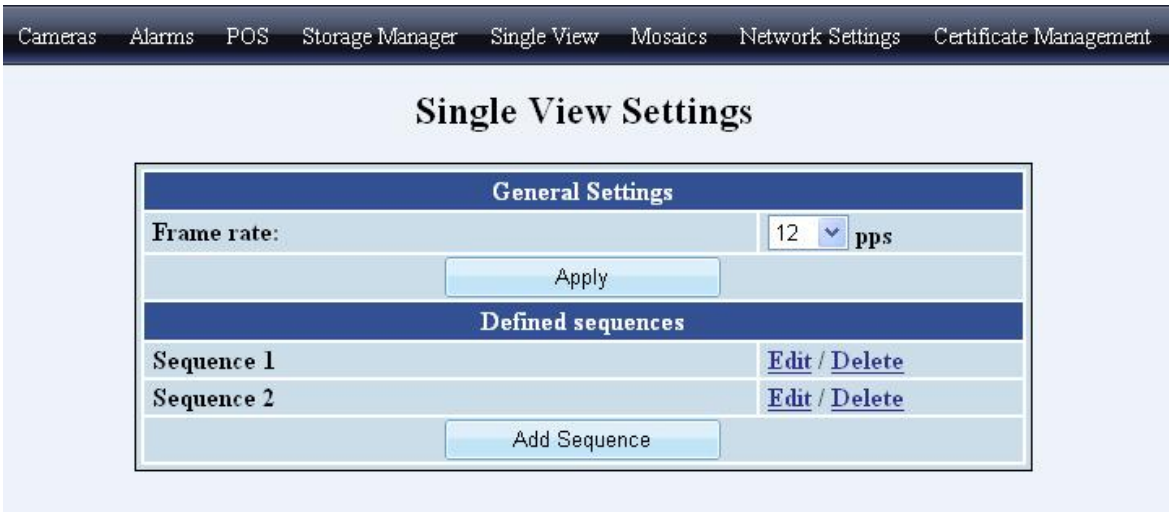
Requesting the **Detailed Used Storage Information** may take a few minutes. The WebCCTV server examines the disk on the first Detailed Information request only. Since it is cached internally, all requests within the next 10 minutes will produce the same result. A request made after 10 minutes, will restart the information collection process and delivers updated information.

To go back to the Detailed Used Storage Information Screen, click **Return**.

5.3.5 Single View

This menu allows you to configure the settings for the **single camera live viewing mode**. The **Single View** menu contains the following parameters:

- Frame rate
- Sequence



Single View Settings Screen

5.3.5.1 Frame rate

The frame rate set by this parameter is the frame rate for the live view visualisation. The possible **Frame Rate** ranges from 0.5 to 30 fps (frames per second). The real frame rate depends on the available network bandwidth and the camera model. In order to set a desired frame rate follow the steps below:

1. Select the frame rate value from the drop-down list.
2. Click the **Apply** button.

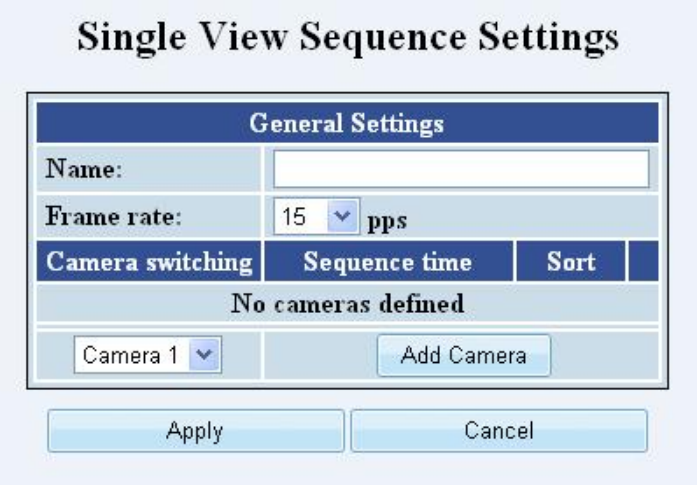
It is recommended to test the various settings in order to choose the optimal Frame Rate and the desired quality of the image.

By default the live view frame rate is 12 fps.

5.3.5.2 Sequence

The **Camera Switching Sequence** allows you to create a sequence of cameras in which cameras will switch in a defined order after a certain time interval set for every camera independently.

You are able to create different sequences with different settings. To add a sequence, click **Add Sequence** button. The following screen will be opened:

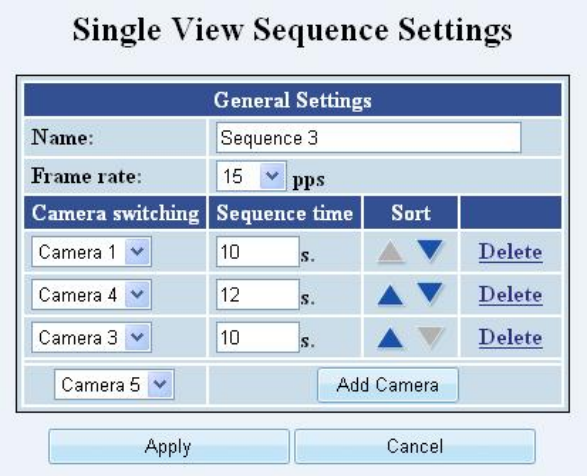


Single View Sequence Settings Screen

The Camera Switching Sequence setting allows the adding or removing of cameras at any time. This allows you to dynamically monitor the most significant areas.

The sequence time option defines the duration of the interval between each camera view.

To **edit** or **configure** a sequence, click the **Edit** link and follow the steps below:



Single View Sequence Settings Screen

1. Specify a **Name** for the sequence.

2. Select **Frame rate**.
3. Add cameras to the sequence:
    a. Select a camera from the drop-down list.
    b. Click the **Add Camera** button.
    c. Specify the **Sequence time** for every camera.

Sequence time for a camera is the time span during which WebCCTV shows this camera.

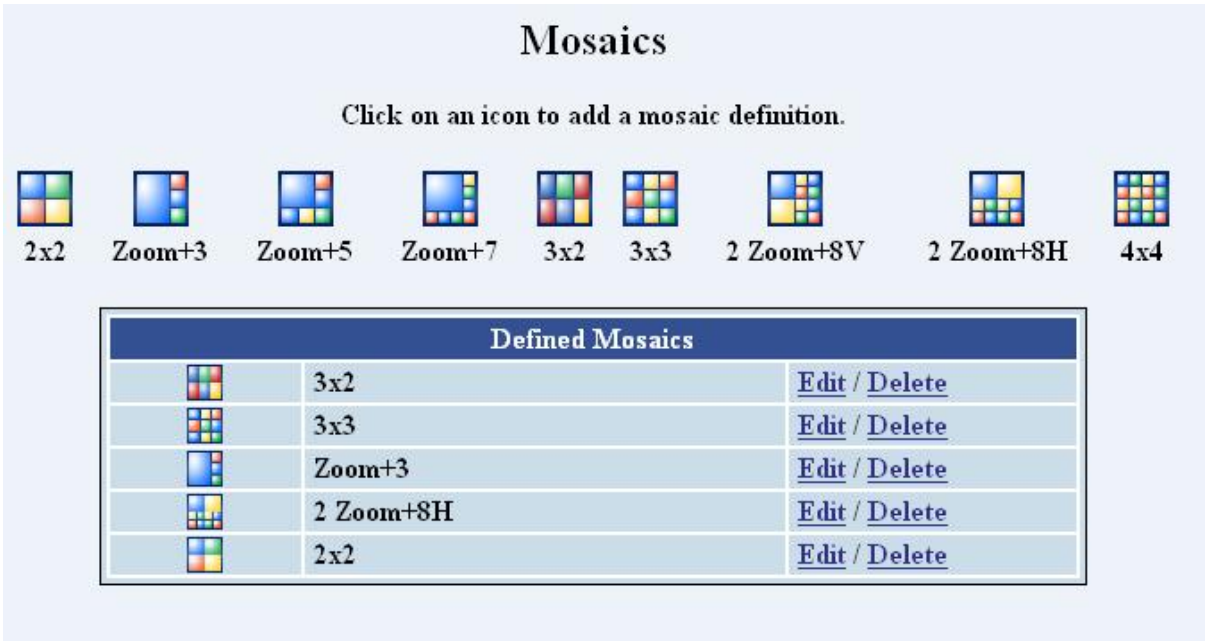
    d. Use the **Sort** buttons to change the position of a camera in the sequence.

To delete a camera, click the **Delete** link.

    e. Click the **Apply** button. You will return to the Single View Settings Screen.

5.3.6 Mosaics

This menu allows you to configure the settings for the **mosaics viewing mode** which provides enhanced surveillance capabilities as you can monitor video from several cameras on one screen simultaneously. This chapter explains how to add and configure the mosaic views in WebCCTV.



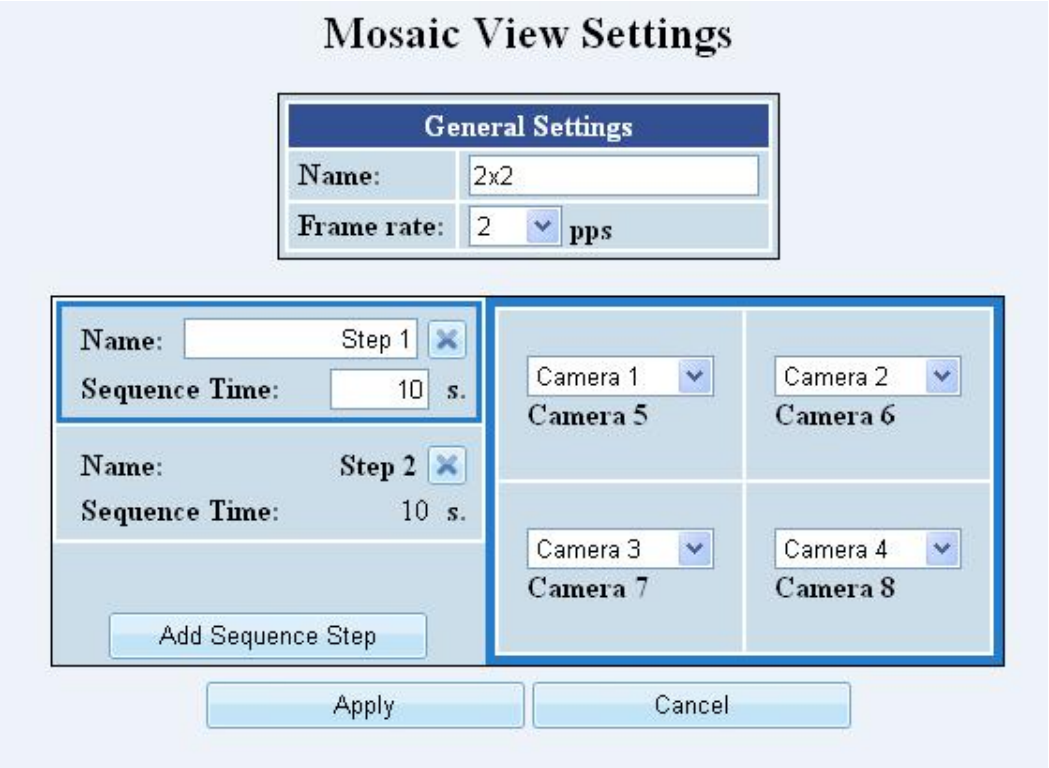
Mosaic Menu Screen

To **add** a mosaic, choose one of the 9 available mosaic views by clicking on the icon of the desired mosaic view. The mosaics view will be added to the list of **Defined Mosaics**.

There are **9** available **mosaic views**:

2x2	A square with two images on top and two below.
Zoom+3	One of the images appears large, and three others are small.
Zoom+5	One of the images appears large, and five others are small.
Zoom+7	One of the images appears large, and seven others are small.
3x3	A square with three times three images.
3x2	A square with two times three images.
2 Zoom + 8V	Two of the images appear large, and 8 others are small at the left.
2 Zoom + 8H	Two of the image appears large, and 8 others are small at the bottom.
4x4	A square with four times four images.

To **Edit** or **configure** a mosaic view, click the **Edit** link and follow the steps below:



Mosaic View Settings Screen

1. Specify a **Name** for the mosaic.
2. Select the **Frame rate**.
3. Configure **Sequence**:
    a. Select cameras from the drop-down lists.
    b. Specify a **Name** for the sequence (step).
    c. Specify **Sequence time**.

Sequence time is the time (in seconds) that is used to switch between all sequences (steps). This is only relevant when two or more sequences (steps) are configured.

4. Add additional Sequences (optional).

Frame rate is the number of frames shown per second. This setting only applies to the focus view, the small views by default have 1 fps as frame rate.

5. Click the **Apply** button.

By default each mosaic view is created with the number of steps needed to involve all available cameras.

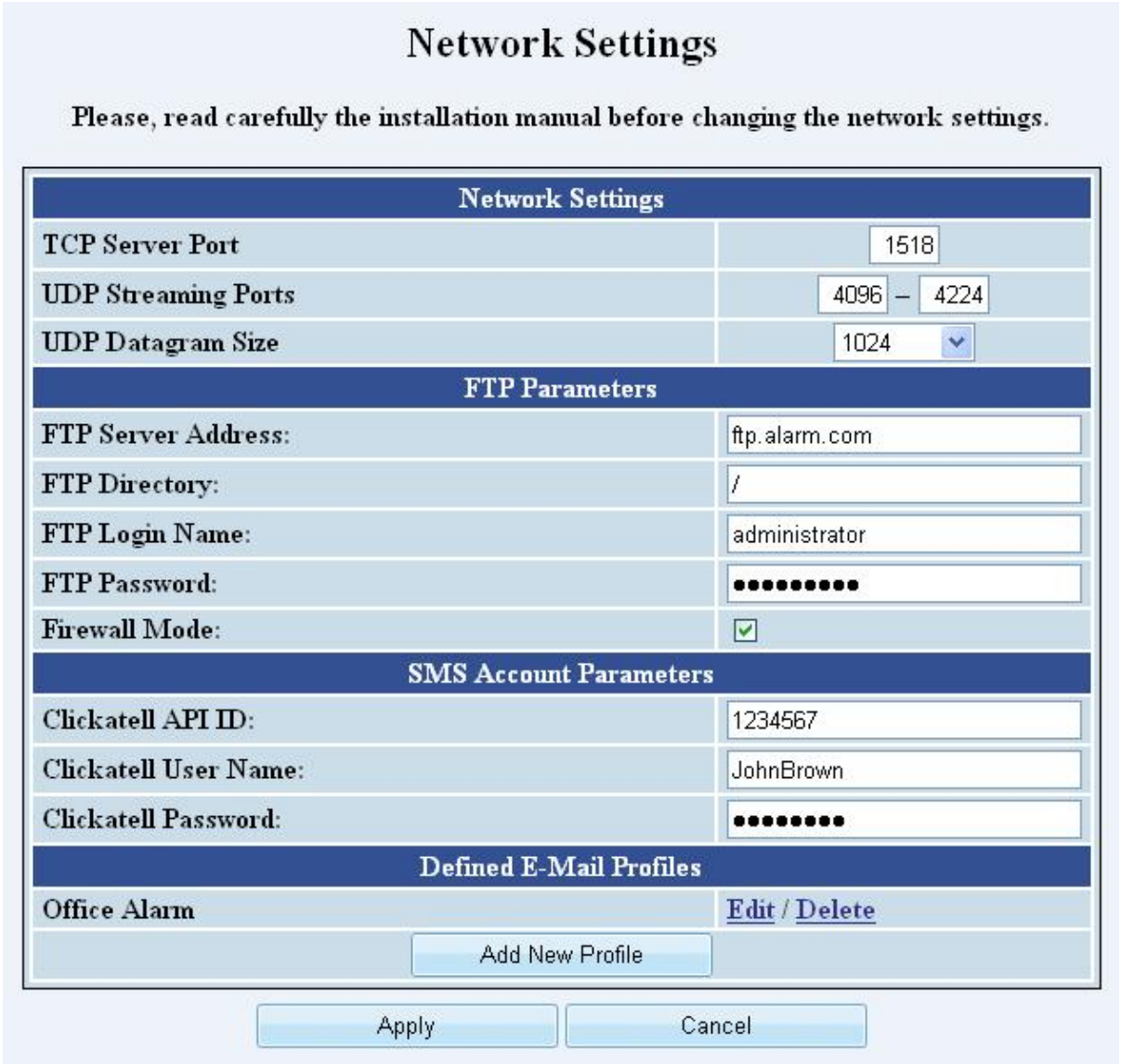
You can delete a Step any time by clicking the **Close** button in the upper right corner of the Sequence (step) section.

To go back to the Mosaics Screen, click the **Cancel** button.

5.3.7 Network Settings

This chapter explains how to change the WebCCTV server's network settings. The following settings are described:

- Network settings
- FTP Parameters
- SMS Account Parameters
- E-Mail Profiles



Network Settings Screen

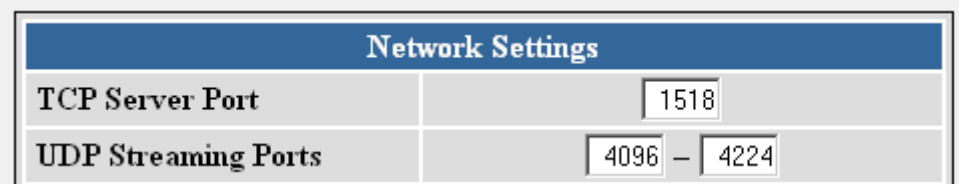
Don't change any parameter unless you are absolutely sure.

The FTP Parameters, SMS account Parameters and Defined E-Mail Profiles sections are only visible when the WebCCTV Alarm Component is installed.

5.3.7.1 Network settings

The following parameters can be configured:

- **TCP Server Port** – port which is used to allow external users to receive alarms, control PTZ cameras, send commands, etc. This is called the WebCCTV control signal.
- **UDP Streaming Ports** – ports used to transmit video streams. WebCCTV chooses the necessary amount of ports from the range 4096 - 4224 to transmit video streams.
- **UDP Datagram Size** – size of the packets (datagrams) on which the video stream is divided for proper transmission over the network. This parameter is measured in bytes.



Network Settings Screen

Click the **Apply** button to save the settings.

5.3.7.2 FTP Parameters

FTP Uploading enables automatic uploading of movies and images, which were recorded or captured when an incoming alarm was triggered, onto a remote FTP server.

This section is only present if the WebCCTV Alarm Component is installed.

Following parameters can be configured:

- **FTP Server Address** – address of the FTP server.
- **FTP Directory** – directory used for storing the uploaded movies and images.

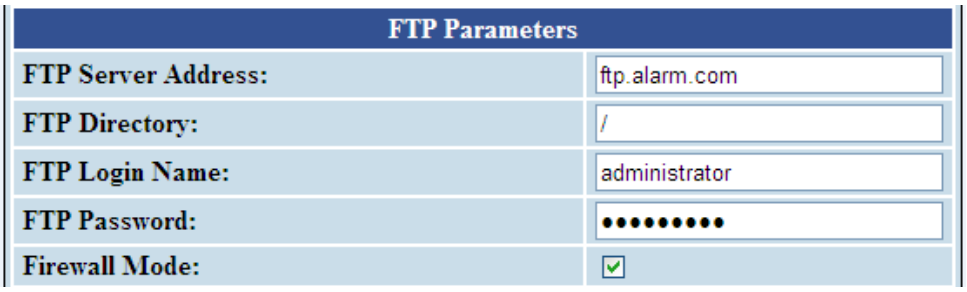
To upload alarm movies and images to the FTP server's root directory specify the slash sign (/) in the FTP Directory field.

- **FTP Login Name** – name used to logon to the FTP server.
- **FTP Password** – password used to authenticate the user on the FTP server.

Contact your FTP server administrator to obtain your FTP Login Name and FTP Password.

- **Firewall Mode** – check the checkbox if you want to enable this feature.

Firewall Mode allows you to upload alarm movies when the firewall is active.



FTP Parameters Screen

Click the **Apply** button to save the settings.

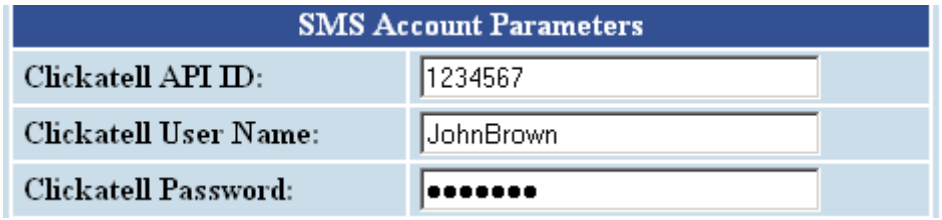
5.3.7.3 SMS Account Parameters

SMS enables automatic sending of SMS message when an incoming alarm was triggered.

This section is only present if the WebCCTV Alarm Component is installed.

The following parameters can be configured:

- **Clickatell API ID** – ID assigned to your Clickatell account.
- **Clickatell User Name** – user name of the Clickatell account.
- **Clickatell Password** – password of the Clickatell account.



SMS Account Parameters Screen

If you don't have a Clickatell account, you can create one by clicking the following direct link: http://www.clickatell.com/developers/api_http.php

Click the **Apply** button to save the settings.

5.3.7.4 E-Mail Profile

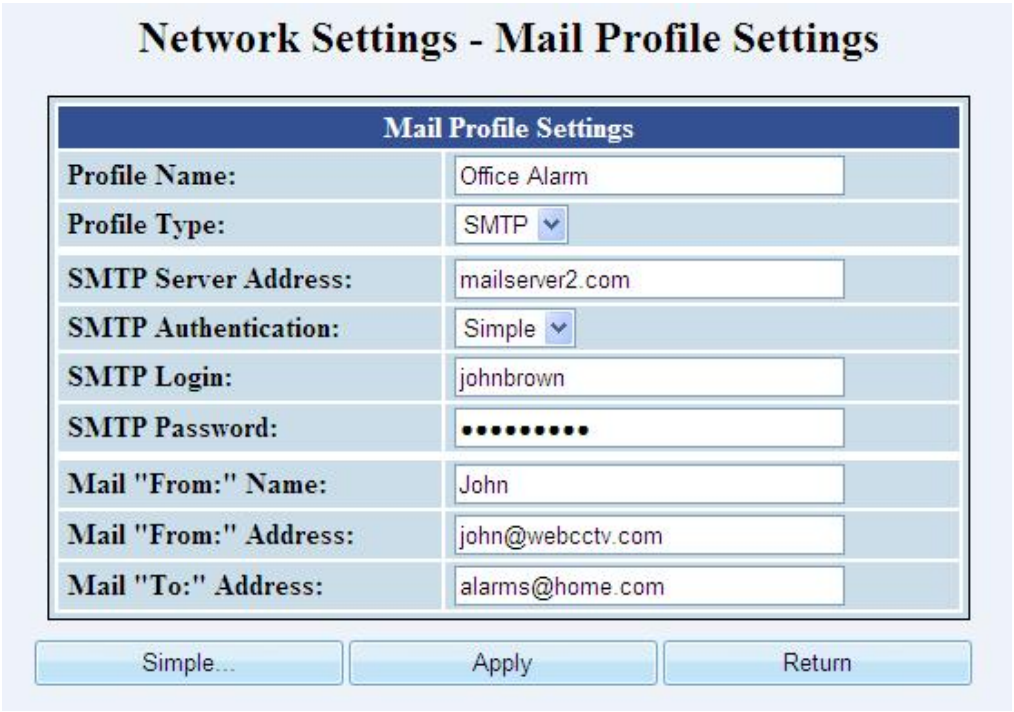
An **E-Mail Profile** is intended for storing email parameters necessary for successfully sending and receiving email notifications of incoming alarms.

This section is only present if the WebCCTV Alarm Component is installed.

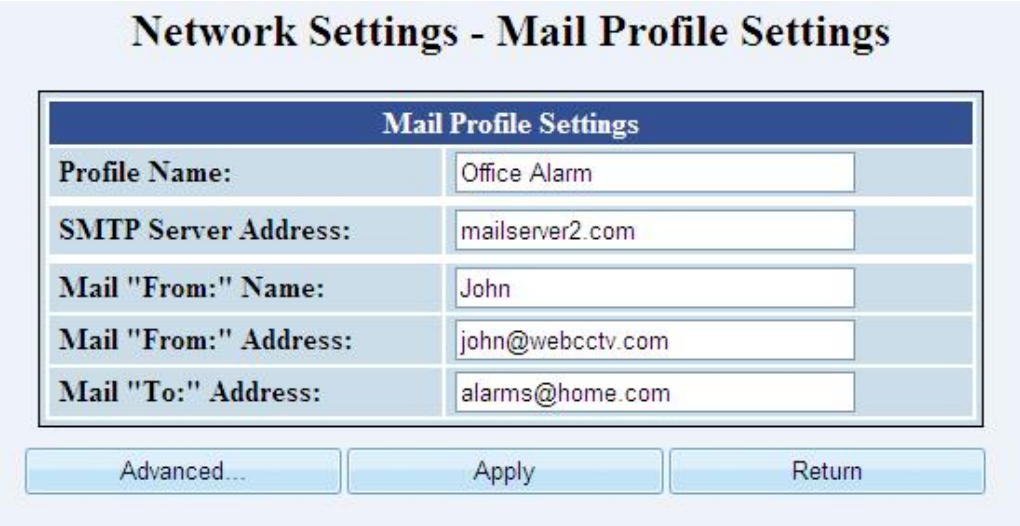
Defined E-Mail Profiles Screen

To **add** the profile, follow the steps below:

1. Click the **Add New Profile** button.
2. Choose the type of Mail Profile mode (**Advanced** or **Simple**), by clicking the appropriate button.



Mail Profile Settings Screen (Advanced Mode)



Mail Profile Settings Screen (Simple Mode)

3. Specify the **Profile Name**.
4. Select a **Profile Type** of mail sending. You can choose out of **Direct** or **SMTP** as mail protocol. (not available in simple mode)

You are able to select two types. Your choice should depend on the capabilities of your mail server (i.e.the location of the server where the mail is stored).

5. Specify the **SMTP server address**.
6. Select type of **SMTP authentication**.

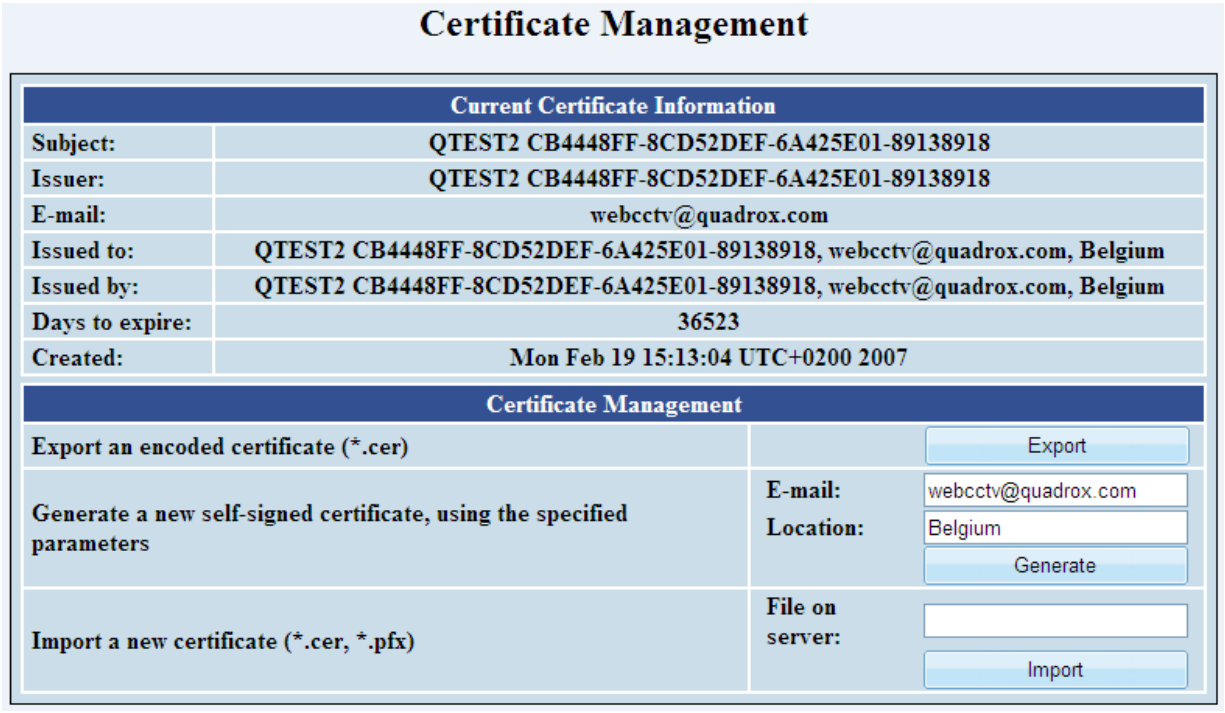
Most SMTP servers don't use authentication for sending mail, please confirm the setup of the SMTP server you use. If you encounter a problem with sending mail via an SMTP server, test sending an alarm mail both with and without authentication.

7. Specify **SMTP Login**.
8. Specify **SMTP Password**.
9. Fill in the **"Mail:" From: Name:** field with the name you want to display in the **From** field of the alarm mail.
10. Fill in the **"Mail:" From: Address:** field with the address from which the alarm mail will be sent.
11. Fill in the **"Mail:" To: Address:** field with the address to which the alarm mail will be sent.
12. Click the **Apply** button to save the settings.

To go back to the Network Settings Screen, click the **Return** button.

5.3.8 Certificate Management

The **Certificate Management** section allows you to handle your certificates for exported movie signing.



Certificate Management Screen

The **Current Certificate Information** section consists of general information about the certificate which is currently used by WebCCTV for export movie signing, such as:

- Name of your certificate
- Certificate name of an issuer which signed your certificate
- Email you specified for certificates generating
- Complete ithe nformation that identifies your certificate (including name, email and location)
- Complete the information that identifies the certificate of an issuer which signed your certificate (including name, email and location)
- Days left to your certificate expiration
- Date of your certificate generation

Subject/Issuer and **Issued to/Issued by** fields are the same if using a self-signed certificate.

5.3.8.1 Self-signed certificates

During the WebCCTV installation a self-signed certificate is created which has non-personalized information. It is recommended that you create a new certificate which will include your information as a signer. To do that, follow the steps below:

1. Specify your e-mail in the **E-mail** field.
2. Specify your location in the **Location** screen.
3. Click the **Generate** button.

Your new self-signed certificate has been generated. From now on it is used for signing the export movie files.

To export this certificate for transmitting it to a remote location or other purposes, click the **Export** button and define the location to store.

Self-signed certificates have the following advantages and disadvantages:

Advantages:

- Certificate can be renewed at one's choosing
- Custom information (i.e. location of the recorder and contact email, etc.) which is useful in court can be added
- Certificate doesn't expire
- Certificate is free of charge

Disadvantages:

- Certificate is not verified by a 3rd party, so it has limited trust.
- Certificate should be explicitly added to the trusted certificates list on each machine for the verification.

5.3.8.2 CA signed certificates

In spite of the self-signed certificates advantages, this approach is not the most secure. To improve your security, Quadrox recommends getting a certificate from a trusted certification authority (CA). There are Certification Authorities (CA) which are explicitly trusted worldwide so Microsoft pre-installed theirs certificates in the Windows Operating System. Hence those certificate authorities are trusted by all 3rd parties which use a Windows Operating System. If you get a certificate signed by the CA, you automatically become a trusted signer in the Windows environment.

To import the CA certificate in the WebCCTV system, follow the steps below:

1. Save the certificate on your WebCCTV server.
2. Specify the exact path to the certificate in the **File on server** field.
3. Click the **Import** button.

Exported movie files will now be signed by the imported CA certificate. The main advantage is that you don't need to install it on each machine since this certificate is pre-installed there.

A certificate loses its "trust value" over time, because the longer it is in place, the higher chance it has of being compromised. It is recommended that certificates are renewed regularly and that the old certificate is allowed to expire.

CA certificates have the following advantages and disadvantages:

Advantages:

- Certificate is checked by trusted a 3rd party for maximal security
- Certificate doesn't need to be explicitly added to the trusted certificates list
- Certificate expires

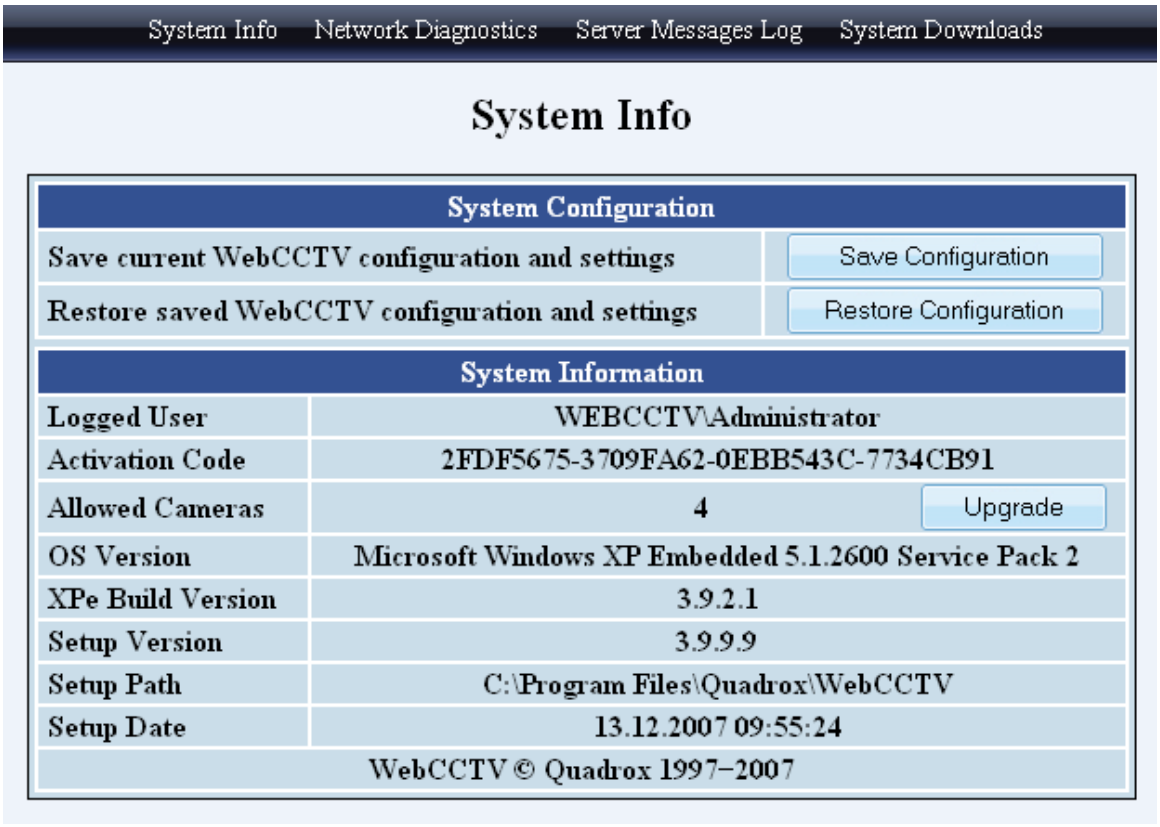
Disadvantages:

- Certificate must be purchased

5.4 Info

The **Info** section gives you detailed information about the WebCCTV Server. The following topics are described in this chapter:

- System info
- Network Diagnostics
- Server Messages Log
- System Downloads

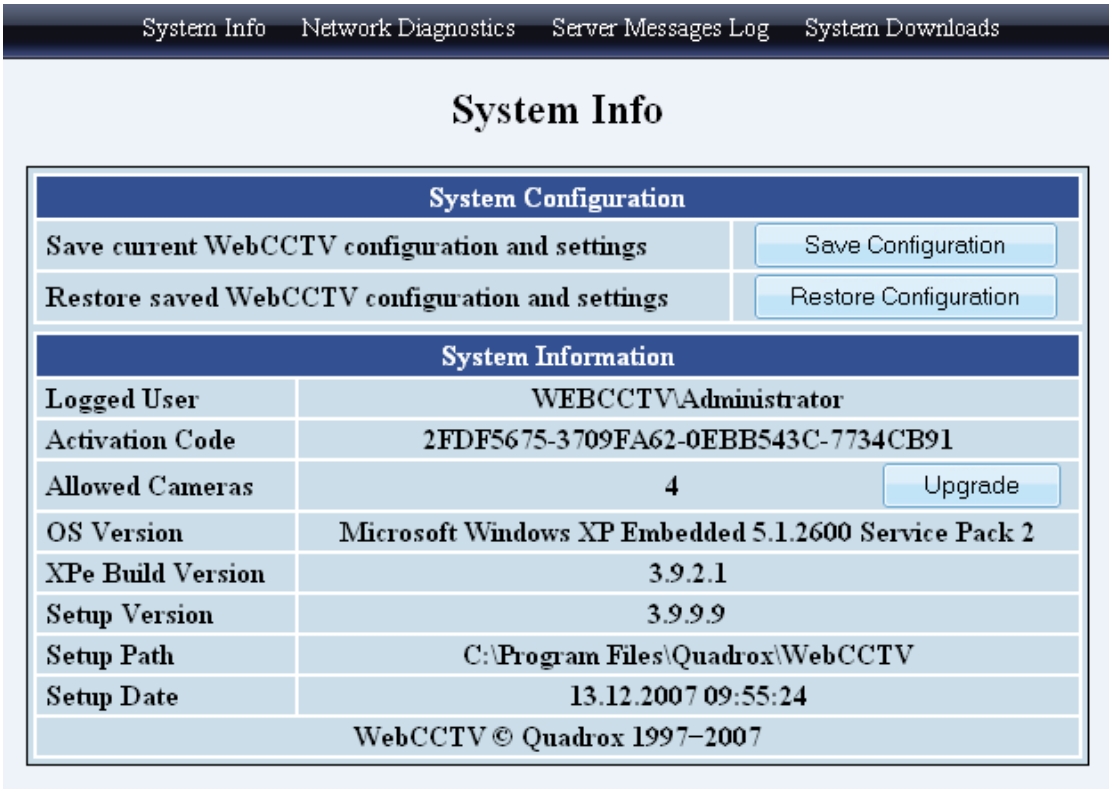


Info Screen

5.4.1 System Info

The System Info screen consists of two sections:

- System Configuration
- System Information



System Info Screen

5.4.1.1 System Configuration

All system configurations can be backed up to an external xml file for backup purposes.

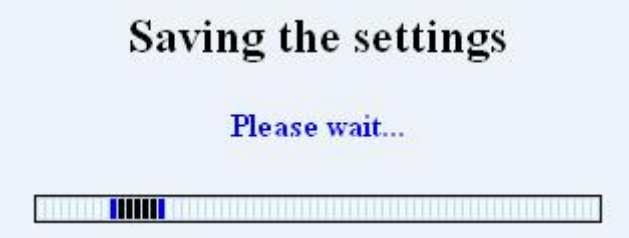
You need to have Microsoft .NET Framework 2.0 installed in order to Save/Restore your configuration. If the Microsoft .NET Framework 2.0 is not installed on your computer, the Save/Restore feature will be unavailable. You can install the standalone Save/Restore functionality from a stand-alone installation setup (refer to ***3.4.4 System Downloads***).

You can save and restore a configuration only if your old software version is 4.0.0.0 or higher. Previous versions can't be restored.

5.4.1.1.1 Saving Configuration

To save the configuration, follow the steps below:

1. Click the **Save Configuration** button**.** The Save/Restore functionality will collect all configuration information.



Saving Settings Screen

2. You will be asked to save an .xml configuration file. Select a directory of your choice and click the **Save** button.

You need Microsoft .NET Framework 2.0 to be installed in order to Save your configuration.

5.4.1.1.2 Restoring Configuration

To restore a configuration, follow the steps below:

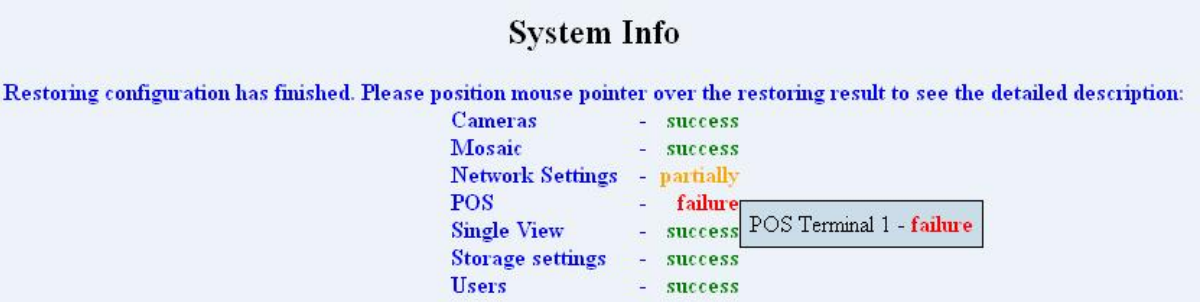
You need Microsoft .NET Framework 2.0 to be installed in order to Restore your configuration.

1. Click the **Restore Configuration** button.
2. Choose a saved configuration .xml file.
3. Click **Open**.

After restoring the configuration, all passwords of any users added to WebCCTV will be defaulted to the following password: **videouser.** It is strongly recommended to change all these passwords.

While restoring a configuration the WebCCTV Server may restart several times. This is a normal behavior. Please be patient until the restoring process is finished.

When the restoring process is finished, an overview will be given outlining the results of your restore action. In case a particular section was not (or partially) restored, it will be marked in yellow or red. Move the mouse cursor over the results in order to see the detailed information of that section.


System Info
Restoring configuration has finished. Please position mouse pointer over the restoring result to see the detailed description:
Cameras - success
Mosaic - success
Network Settings - partially
POS - failure
Single View - success
Storage settings - success
Users - success
POS Terminal 1 - failure

Restore Results Screen

5.4.1.2 System Information

The System Information section describes the following parameters:

- **Logged User** – user that is logged in.
- **Activation Code** – activation code based on the machine and number of allowed cameras.

When reinstalling or upgrading the WebCCTV software on the same machine, you can reuse the Activation Code as long as crucial components as CPU, Motherboard or Network Interface Card aren't replaced. The Hard disk is not a crucial component.

It's possible that the Activation Code is invalid if you have two different Network Interface Cards installed on your machine. The Activation Code is based on one NIC (Network Interface Card).

You can Upgrade your license in order to be able to monitor more cameras. Click the **Upgrade** button in the **Activation code** row. You will be redirected to the Activation page where you should specify the new key. To obtain this key, contact Quadrox or your installer.

- **Allowed Cameras** – specifies the number of cameras that may be connected to the system.

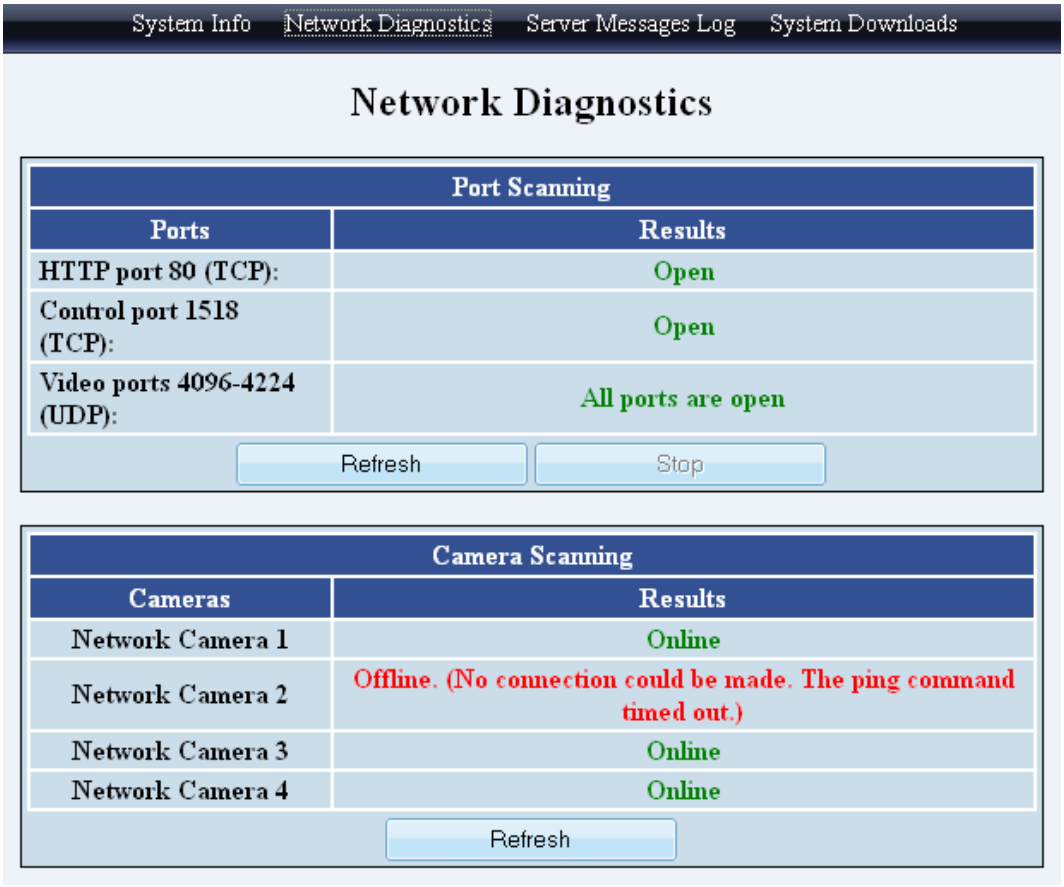
You can connect as many cameras as you like to the system, but only the number of allowed cameras will be active. The system automatically selects which cameras are active . At first, analogue slots will be replaced by network cameras if analogue cameras are present. If all cameras are network cameras, there will be a selection based on an internal mechanism.

- **OS Version** – version of the operating system that is installed.
- **XPe Build Version** – build version of the XPe operating system.
- **Setup Version** – WebCCTV software version installed.
- **Setup Path** – directory where the WebCCTV software is installed.
- **Setup Date** – date of installation.

5.4.2 Network Diagnostics

This section allows you to check the state of the ports (opened/closed) necessary for proper operation of the software. It consists of two diagnostic functionalities:

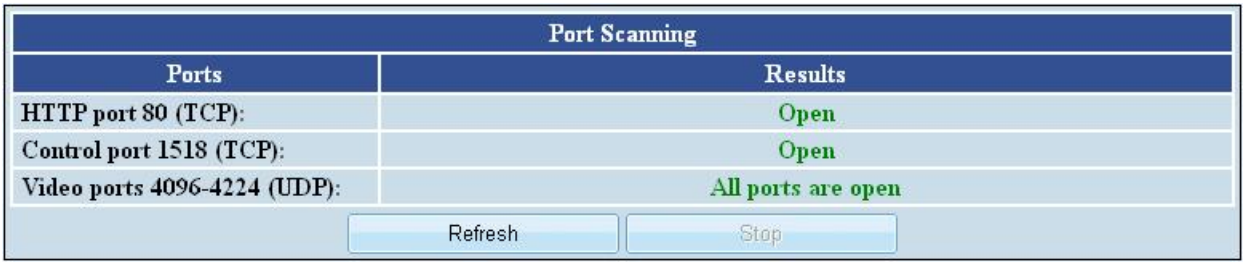
- Port Scanning
- Camera Scanning



Network Diagnostics Screen

5.4.2.1 Port Scanning

The **Port Scanning** feature allows you to check the state of the **TCP** and **UDP ports** needed for a normal server operation. When entering the Network Diagnostics page, all ports are checked automatically.



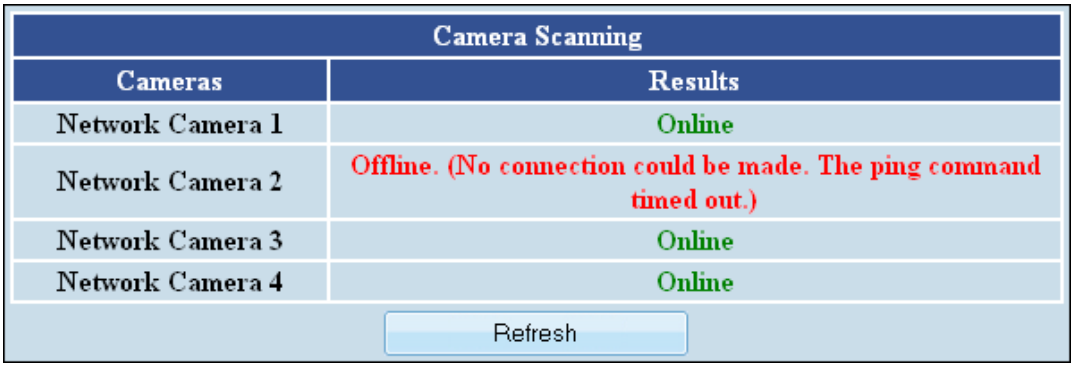
Port Scanning Screen

These ports also have to be configured in your firewall(s) and router port forwarding if you want to connect to your server over the Internet.

Click the **Refresh** button if you want to refresh the status of the ports.

5.4.2.2 Camera Scanning

The **Camera Scanning** feature allows you to check the connection status of the cameras connected to the system. When entering the Network Diagnostics page, all cameras are checked automatically.



Camera Scanning Screen

The camera can have two states:

- Online
- Offline

Only network cameras will be shown in the Camera Scanning list.

Click the **Refresh** button if you want to refresh the status of the cameras.

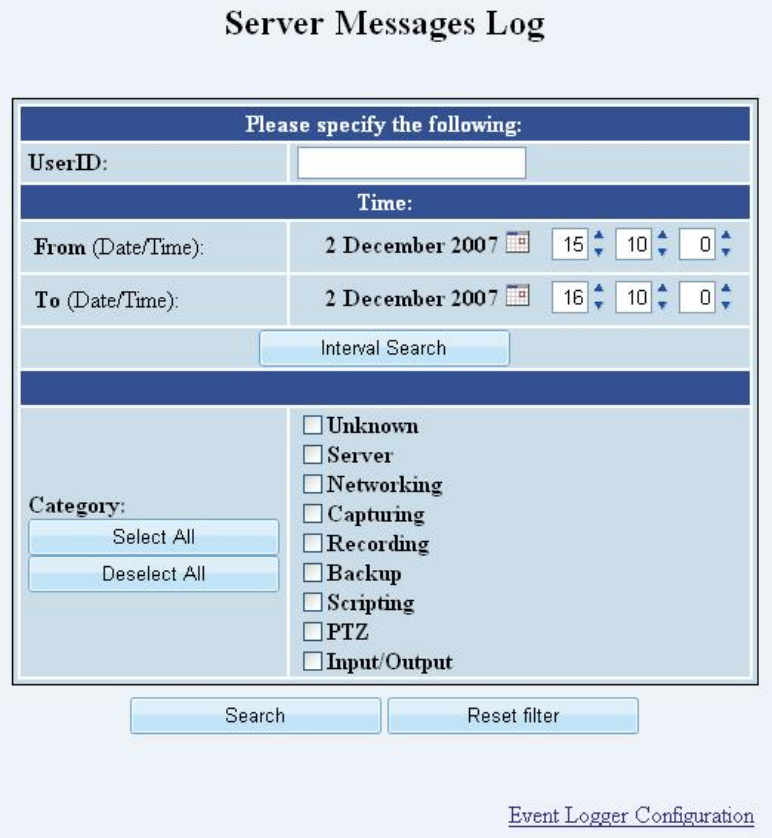
5.4.3 Server Messages Log

WebCCTV stores all server actions in its Server Messages Log. Examples of server messages are capturing, recording, backup, etc. This log is kept inside the Windows operating system itself. Technically, it is kept inside a specific WebCCTV event log container in the Windows event logging subsystem.

The amount of logged server actions (number of days contained in the log) depends on the defined size of the event viewer. In normal circumstances, the log is large enough to keep WebCCTV server logs for approximately 60 days.

5.4.3.1 Log Search

The search option allows you to retrieve all or specific actions that have been performed on the server.



Server Messages Log Screen

All possible actions are described in the following table and can be found in the picture above.

Category	Description
Unknown	Actions and errors from an unknown source.
Server	Starting and stopping of the server.
Networking	Actions concerning the network connections.

Capturing	Actions concerning image acquisition.
Recording	Actions and errors concerning recordings.
Backup	Cleaning up of old video footage files.
Scripting	Script messages.
PTZ	Movements and settings from PTZ.
Input/Output	Changes in the in- and outputs settings.

To do a search, follow the steps below:

1. Specify the user for which you want to search (Optional).
2. Define the time frame in which you want to search.
3. Check the required categories checkboxes.
4. Click the **Search** button.

The figure below provides a sample overview of a Server Messages Log.

Server Messages Log

Type	Time	Category	User	Description
	19.02.2007 16:58:39	Backup	SYSTEM	Backup was stopped after having cleaned up 146 MB amounting to 493 MB available disk space.
	19.02.2007 16:58:37	Backup	SYSTEM	Backup was started due to 'free disk space limit' with 347 MB of free disk space.
	19.02.2007 16:53:41	Server	SYSTEM	Server successfully started.
	19.02.2007 16:53:31	Server	SYSTEM	Server successfully stopped.
	19.02.2007 16:53:20	Server	pysanets	User requested restart of the service.
	19.02.2007 16:50:43	Backup	SYSTEM	Backup was stopped after having cleaned up 169 MB amounting to 492 MB available disk space.
	19.02.2007 16:50:42	Backup	SYSTEM	Backup was started due to 'free disk space limit' with 322 MB of free disk space.
	19.02.2007 16:10:46	Server	SYSTEM	Server successfully started.
	19.02.2007 16:10:36	Server	SYSTEM	Server successfully stopped.
	19.02.2007 16:10:25	Server	pysanets	User requested restart of the service.
	19.02.2007 15:51:11	Server	SYSTEM	Server successfully started.
	19.02.2007 15:41:19	Server	SYSTEM	Server successfully stopped.
	19.02.2007 15:26:23	Server	SYSTEM	Server successfully started.
	19.02.2007 15:26:17	Server	SYSTEM	Server successfully stopped.
	19.02.2007 15:26:06	Server	pysanets	User requested restart of the service.
	19.02.2007 15:21:17	Server	SYSTEM	Server successfully started.
	19.02.2007 15:21:11	Server	SYSTEM	Server successfully stopped.
	19.02.2007 15:20:57	Server	pysanets	User requested restart of the service.
	19.02.2007 15:20:37	Server	SYSTEM	Server successfully started.
	19.02.2007 15:20:31	Server	SYSTEM	Server successfully stopped.

160 match(es) found Page 1 2 3 4 5 ... 8

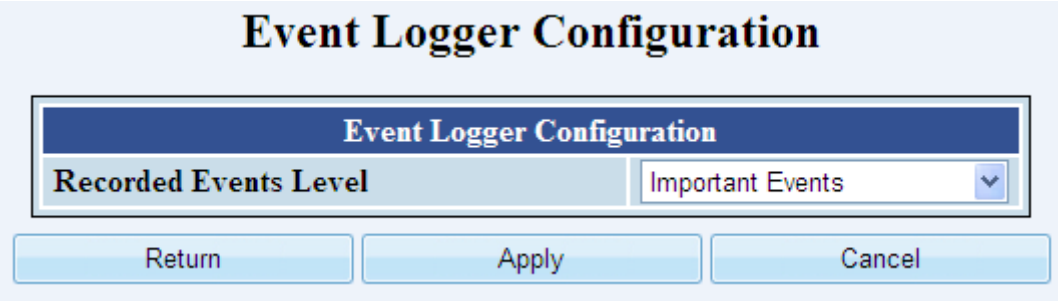
Server Messages Log Result Screen

The Server Messages Log allows you to check all server related actions by users at all times.

In order to conduct a new log search, click on the **New search** button. The reset filter button will clear all the checked boxes so that you can make a new selection.

5.4.3.2 Event Logger Configuration

The Event Logger Configuration defines the priority levels for the recorded events. Depending on the selected option, WebCCTV will or will not store certain events.



Event Logger Configuration Screen

There are three Recorded Events levels:

- **Only Critical Events** – WebCCTV stores the most important system events that occur when proper WebCCTV performance is impossible, e.g. recording break, failure to detect a system component, etc.
- **Important Events** – WebCCTV stores system events labelled as "Only Critical Events" and system events that play a significant role in the WebCCTV operating, e.g. playback stream creating, system logging on, etc.
- **All Events** – WebCCTV stores all system events.

To apply the new settings, click **Apply**.

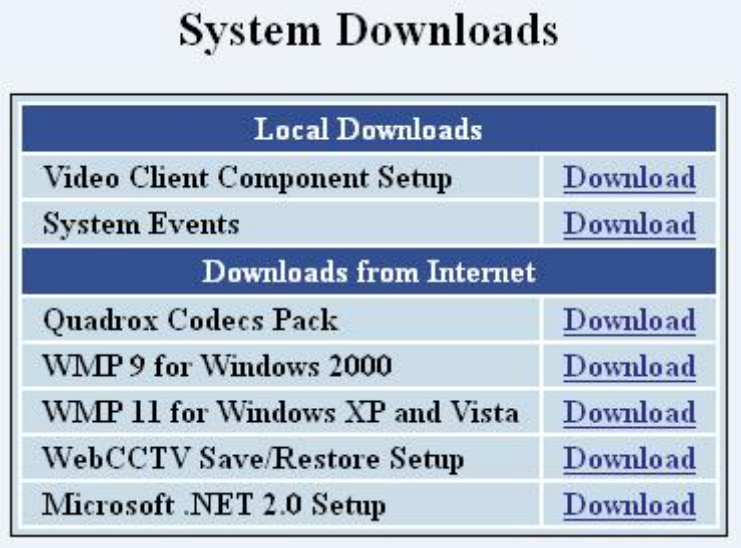
To cancel your changes, click **Cancel.**

To go back to the Server Messages Log screen, click **Return**.

Event Logger Settings functionality is unique for both User Actions Log and Server Actions Log.

5.4.4 System Downloads

The **System Downloads** section allows you to download software or installation files that may be needed on your system depending on the functionalities you are using or want to use.



System Downloads Screen

The following items are downloaded from the WebCCTV Server **(Local Downloads)**:

- **Video Client Component Setup** – installation setup which deletes "old" ActiveX's and installs the one for your current WebCCTV installation.
- **System Events** – all event logs. This can be requested for support purposes.

The following items are downloaded from the **Internet**:

You must be connected to the Internet.

- **Quadrox Codecs Pack** – enables you to view Live Streams and playback Recordings in MPEG 4 format created by the WebCCTV software.
- **WMP 9 for Windows 2000** – standard Windows 2000 player which may be needed in order to play exported movies.
- **WMP 11 for Windows XP and VISTA** – latest version of Windows Media Player which is XP and Vista compatible. May be needed in order to play exported movies.
- **WebCCTV Save/Restore Setup** – standalone installation setup for the WebCCTV Save/Restore functionality.
- **Microsoft .NET 2.0 Framework** – pack of libraries needed for some WebCCTV components (Alarms, Save/Restore etc.).

6 Video Browser

This chapter provides an overview of the WebCCTV Video Browser Control Panel and the following WebCCTV functions:

- Live
- Recordings
- Alarms
- POS

6.1 Video Browser Control Panel

Network status indicator
The green dot, in the top left corner, indicates a good network status. When the indicator is red, the WebCCTV is experiencing network problems which can result in slow response from the Web Application or no response at all.

Live
Click this button to access the Live View menu where you can see streaming from all your cameras and control PTZ cameras.

Recordings
Click this button to access the Recordings menu where you can export recorded movies or search recordings including alarm and POS transactions.

Alarms
Click this button to access the Alarms menu where all alarms are centralised together with their associated recordings including an export feature.

Hide Control Panel
Click this button to hide or retrieve the control panel**.**

POS
Click this button to access the POS menu where all POS transactions are centralised together with their associated recordings including an export feature.

My Account
Click this button to change your password.

Manager
Click this button to open the Video Manager application.

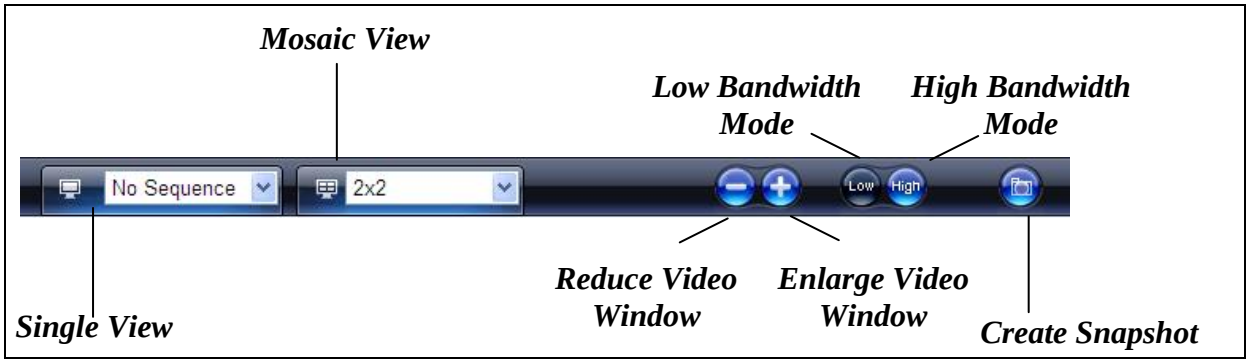
Help
Click this button to access WebCCTV Online help.

Log Off
Click this button to change user.

Exit
Click this button to exit the WebCCTV application.

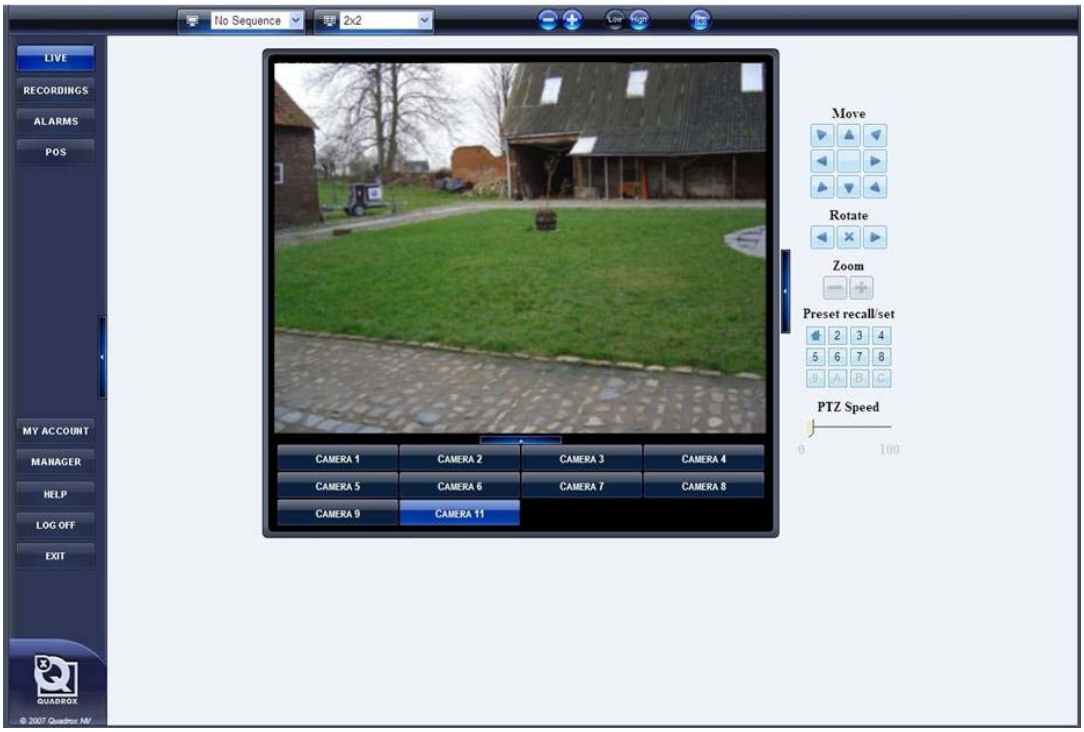
6.2 Live

The WebCCTV Video Browser application allows you to monitor cameras through a comprehensive and user-friendly interface.

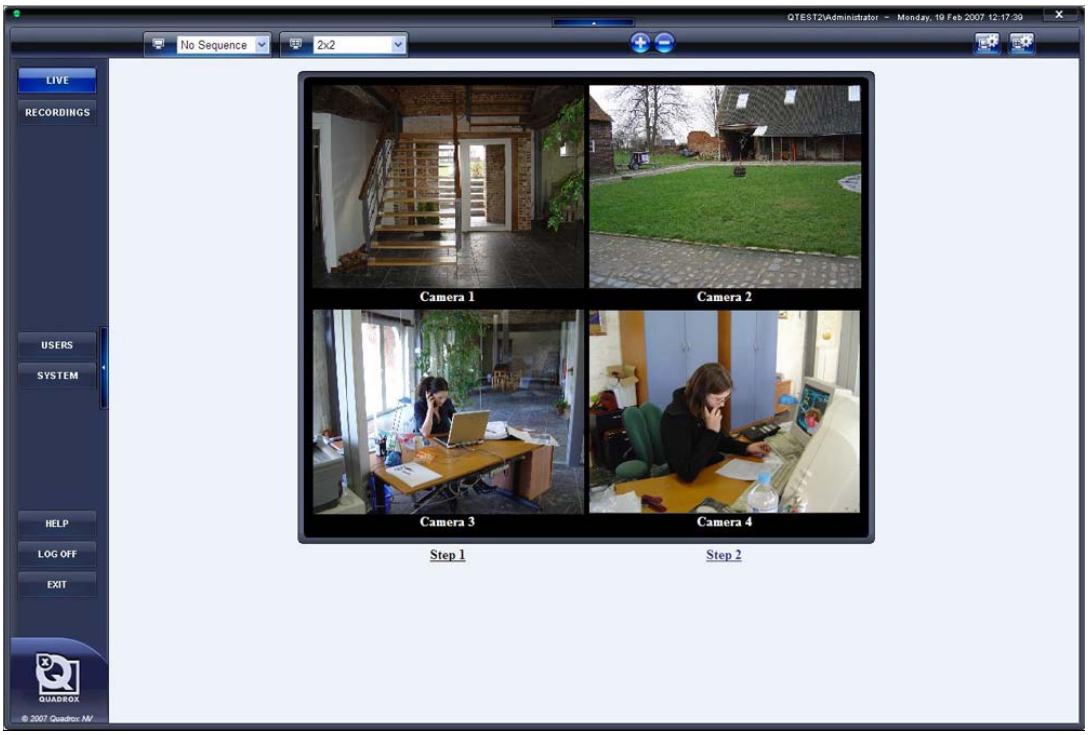


The following features are present in the **Live** menu:

- Single View
- Mosaic View
- Reduce/Enlarge Video Window
- Low/High Bandwidth Mode
- Create Snapshot
- PTZ (optional)
- Digital Zoom
- Audio



Live (Single View) Screen



Live (Mosaic View) Screen

6.2.1 Single View

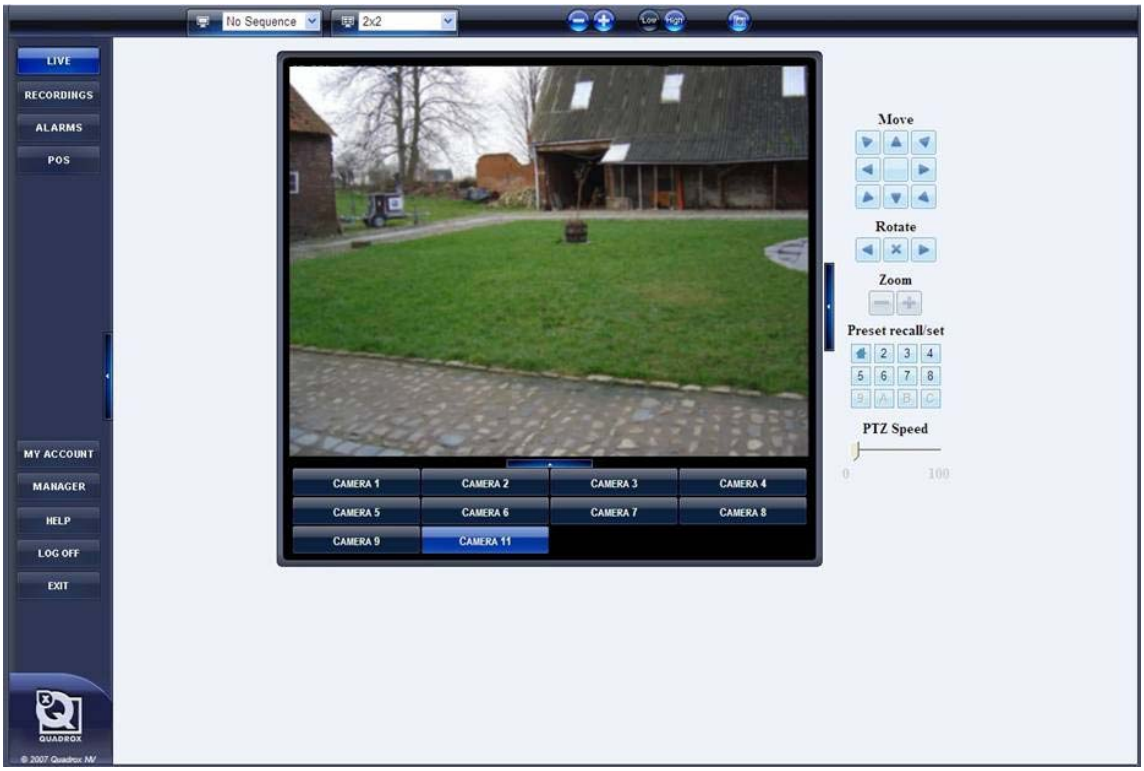
When entering the **Live** menu, single view mode is automatically displayed. In single view one camera is displayed at a time. You can switch between cameras by clicking the corresponding camera buttons below the viewing window. The following features are available in the **Live View** screen:

- Selecting a sequence
- Selecting a mosaic
- Enlarging/Reducing video window
- Selecting high/low bandwidth streaming
- Creating a snapshot
- PTZ functions (optional)
- Digital Zoom
- Audio

Right-click on the video Window to get video streaming parameters such as actual frame rate and dimensions (resolution) of the image.

Use the and buttons to hide the corresponding Single View panels.

The camera you see when accessing Live View is the camera you selected to view the last time you used Live View.



Single View Screen

6.2.1.1 Sequences

To select a Single View Sequence, select the sequence from the drop-down list and click the **Single View** button. If the preferred sequence is already selected in the drop-down list, you can click on at the left of the drop-down list.

Creating sequences can be done in the Video Manager application.

Click on any camera button to stop automatic switching and revert to viewing cameras manually.

When manual switching is completed, automatic switching retakes after 30 seconds.

6.2.1.2 Mosaics

To select a Mosaic, select the mosaic from the drop-down list and click the **Mosaic View** button. If the preferred mosaic is already selected in the drop-down list, you can click on at the left side of the drop-down list.

Creating mosaics can be done in the Video Manager application.

Note that after selecting a mosaic view, the user will automatically be switched to the Mosaic View mode. See ***4.2.2 Mosaic View*** for more information.

6.2.1.3 Changing Video Window Size

You can change the size of the window in which the camera stream is visualized.

Click the button in order to make the Video Window **smaller**.

Click the button in order to make the Video Window **bigger**.

6.2.1.4 Low/High Bandwidth Mode

Low/High bandwidth mode allows you to decide if you want to have streaming video that consumes a reduced bandwidth. You can choose from:

- **High Bandwidth Mode** (Default) – High Bandwidth mode is used preferably on local computers (when the WebCCTV client is located on the same machine as the WebCCTV server), in local area networks or with high-speed Internet connections. Use the **High** ( ) button to enable high bandwidth mode.
- **Low Bandwidth Mode** – Low bandwidth mode is mostly used in medium- or slow-speed LAN or Internet connections. When Low Bandwidth mode is enabled, the frame rate and the resolution of the images are reduced. It produces a reduced bandwidth usage while streaming video. Use the **Low** ( ) button to enable low bandwidth mode.

6.2.1.5 Snapshots

This WebCCTV feature gives you the ability to make snapshots. To create a snapshot, follow the steps below:

1. Choose the frame you want to save and click the button with the camera symbol ( ).
2. Choose the desired location for storing images and click the **Save** button.

Snapshots are saved in .JPEG format.

6.2.1.6 PTZ

WebCCTV supports all standard PTZ functions. These functions are listed below:

Functions	Parameters
Move	left, right, up, down
Rotate	constant left, constant right
Zoom	in, out
Preset recall/Set	select, set
PTZ speed	higher, lower

- **Move** – Using these buttons you can move the camera in any direction you want. To move the camera, click on the button with the arrow pointing in the direction you want to move the camera to.
- **Rotate** – Using these buttons allows you to rotate a dome camera left or right without interruption.

The maximum rotation angle depends on the camera model. Some cameras have a 360° rotation angle, some have less. Check the camera documentation.

- **Zoom** – Click the **"+"** or **"–"** buttons to zoom the image in or out.

Depending on the camera model the zoom function may or may not be present. Check the camera documentation.

- **Preset recall/set** – Using a preset button will instruct the dome camera to jump to a certain predefined position and zoom state. These presets are user-definable. To define a preset setting, move the camera to the position you want, zoom in or out if needed and click one of the buttons while holding the **Ctrl** button on your keyboard. The preset details will then be stored under that number and can be recalled by clicking it (without holding the CTRL key).

Setting presets is only possible if you have Administrator rights.

When the **Home** Preset functionality is enabled, the first preset button is displayed as . This means the camera will return to its Home preset after 300 seconds of inactivity.

- **PTZ Speed** – Function to increase or decrease the camera movement speed.

PTZ Speed is not enabled for PTZ cameras that control the speed themselves.

Please note that using the PTZ functionality within both WebCCTV and the camera software can cause conflicts with the PTZ functionality.

6.2.1.7 Digital Zoom

The Digital Zoom functionality is very useful when there are small details in the scene, but the camera doesn't support optical zoom and there's no way to visually enlarge those objects.

In order to use the Digital Zoom functionality, follow the steps below:

1. Click on the video window in order to set a focal point.
2. Use the mouse wheel to zoom the image in and out (a magnifying glass is shown).
3. When partially or totally zoomed in, click any point on the video screen in order to centralize the video window on this point. This also resets the zoom's focal point.

You cannot use the Digital Zoom functionality if your mouse doesn't have a mouse wheel.

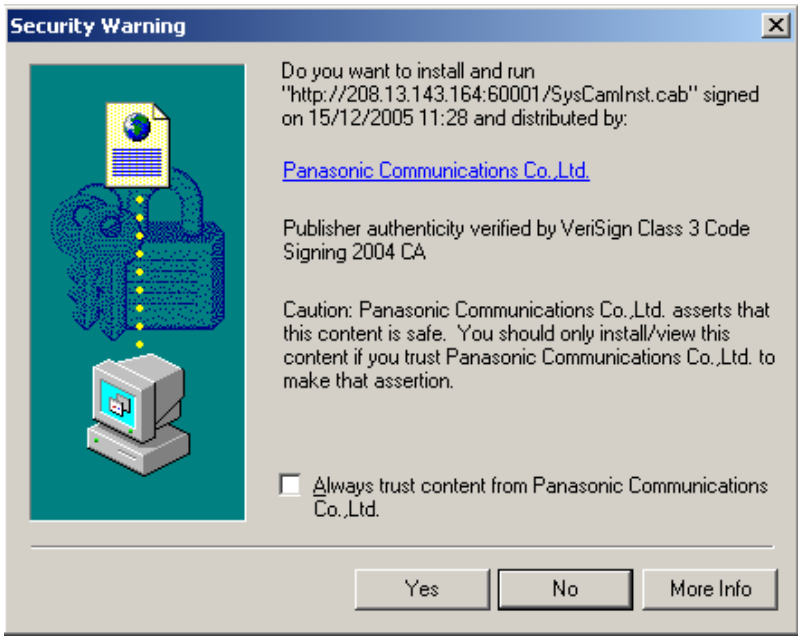
You can use digital and optical zoom simultaneously. You will first zoom optically and switch to digital zoom when you can no longer zoom optically.

6.2.1.8 Audio

WebCCTV supports audio listening for the following Panasonic camera models: BB-HCM311, BB-HCM311A, BB-HCM331, BB-HCM331A, BB-HCM371, BB-HCM371A, BB-HCM381, BB-HCM381A, KX-HCM110, BB-HCE481.

WebCCTV only supports listen-in audio. Recording audio is not available.

To be able to listen to audio, you need to install the **Audio Listening Component** from the camera itself the first time the camera is accessed in Live view. Click the **Yes** button in the dialogue window that appears.


Security Warning
Do you want to install and run "http://208.13.143.164:60001/SysCamInst.cab" signed on 15/12/2005 11:28 and distributed by:
Panasonic Communications Co.,Ltd.
Publisher authenticity verified by VeriSign Class 3 Code Signing 2004 CA
Caution: Panasonic Communications Co.,Ltd. asserts that this content is safe. You should only install/view this content if you trust Panasonic Communications Co.,Ltd. to make that assertion.
Always trust content from Panasonic Communications Co.,Ltd.
Yes
No
More Info

Audio Listening Component Installation Window

After the installation, the **Audio Controls** will appear.

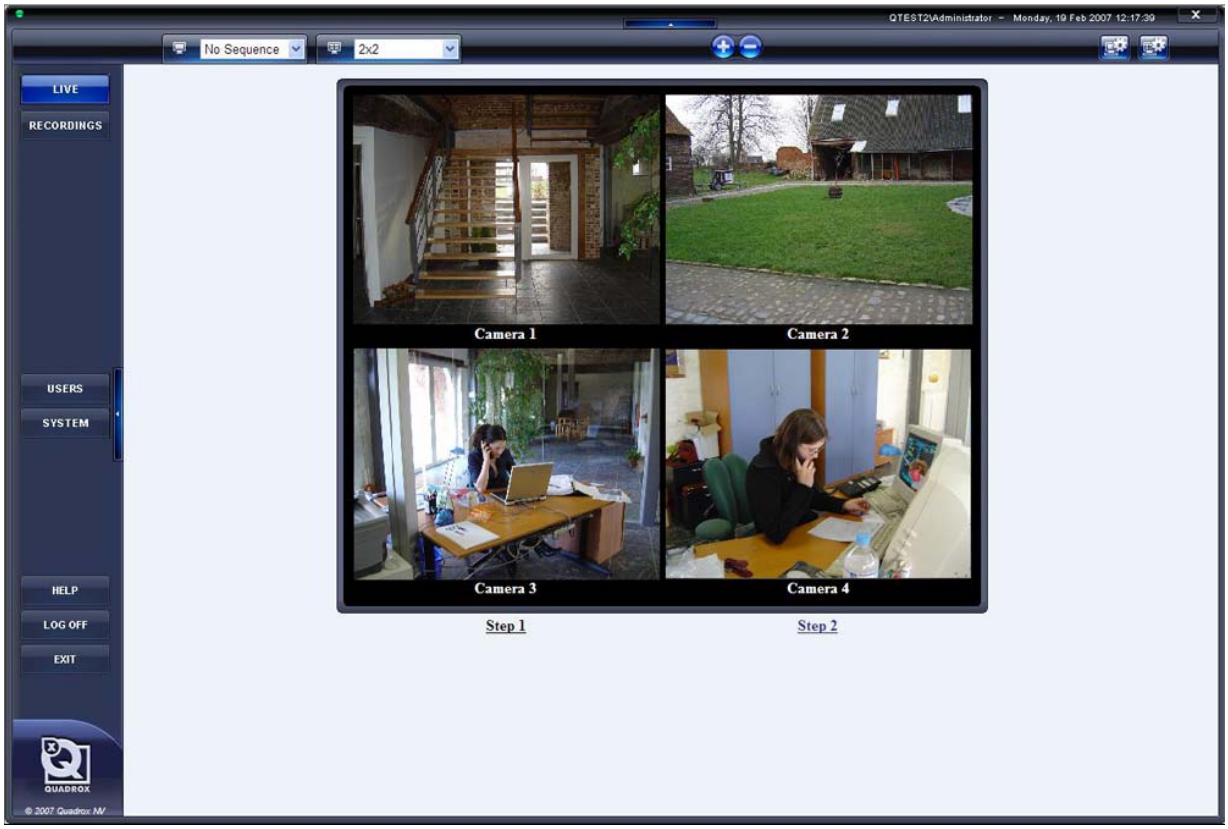
Audio Controls Screen

Figure	Description
	If external speakers are attached to the camera, you can talk to the camera using the PC's microphone. Clicking the button temporarily stops sending audio.
	The audio is stopped. Clicking the button again starts the Talk feature.
	You can listen to the audio around the camera. Clicking the button temporarily stops the audio.
	The audio is stopped.
	This slider adjusts the volume. Sliding to the right increases the volume. Sliding to the left decreases the volume.

6.2.2 Mosaic View

Mosaic View allows you to view up to 16 cameras simultaneously on one screen. This provides enhanced surveillance opportunities and control of all available cameras for a user. The following features are available in the **Mosaic View** screen:

- Selecting a sequence
- Selecting a mosaic
- Enlarging/Reducing video window



Mosaic View Screen

Double click on the video window of a particular camera to switch to the Single View mode for this camera.

When you are using Zoom+3, Zoom+5 or Zoom+7 mosaic views, click on the small camera video windows to move them to the large/central video window. Double click on the central camera video window to switch to the Single View mode for this camera.

The **Snapshots, High/Low Bandwidth**, **Digital Zoom** and **Audio** functionalities are not available in Mosaic View.

6.2.2.1 Sequences

To select a Single View Sequence, select the sequence from the drop-down list and click the **Single View** button. If the preferred sequence is already selected in the drop-down list, you can click on at the left of the drop-down list.

Creating sequences can only be done in the Video Manager application.

Click on any camera button to stop the automatic switching and revert to viewing cameras manually.

When manual switching is completed, automatic switching resumes after 30 seconds.

Note that after selecting a sequence, the view will be automatically switched to Single View mode. See ***4.2.1 Single View*** for more information.

6.2.2.2 Mosaics

To select a Mosaic, select the mosaic from the drop-down list and click the **Mosaic View** button. If the preferred mosaic is already selected in the drop-down list, you can click on at the left side of the drop-down list.

Creating mosaics can only be done in the Video Manager application.

There are 9 predefined mosaic views available for configuration in the Video Manager application. By default, no mosaic view is available in the Video Browser application. In case video capture cards are installed, the respective mosaics will automatically be created and installed by WebCCTV.

6.2.2.3 Changing Video Window Size

You can change the size of the window in which the camera stream is visualized.

Click the button in order to make the Video Window **smaller**.

Click the button in order to make the Video Window **bigger**.

6.3 Recordings

The **Recordings Menu** allows you to search and view recorded footage and export clips of this video footage.

The following sections are described:

- Select Time Period
- Single Playback
- Synchronized Playback
- Alarms
- POS
- Export

POS and Alarms are only available if the **Alarm Component** is installed.

Recordings Screen

6.3.1 Select Time Period

Selecting the time period is needed for all possible recording requests as you need to search amongst all footage which has been recorded.

To select a **time period**, you have to specify the time and date. There are two ways of specifying a certain time period:

1. Using a **From** date and a **Time span** interval: all recorded video footage between the **From** date plus the **Time period**, will be shown.

2. Using **Precise Search** with **From** and **To** date: all recorded video footage between these two points in time will be shown.

Click on the calendar icon to be able to choose the **From** or **To** date.

Click the **Interval search** button in order to return to **Time span** search.

Note that in the **From**/**To** and the **Time span** modes, time and dates in the future cannot be specified. If a date in the future is selected, your time and date will be adjusted to the current date and time.

6.3.2 Single Playback

When using the **Single Playback** feature, you will search among all the recorded video footage for one particular camera. To do this, follow the steps below:

1. Select the time period (see ***6.3.1 Select Time Period***).
2. Check the **Single camera playback** radio button.
3. Choose a **camera** from the drop-down list.
4. Click the **Search** button.
5. For a new single playback recording search, click the **New Search** button.

Recordings Single Playback Screen

When you have the recording mode open, the following functionality is available:

- Single playback controls
- Switching sources
- Activity level
- Slider
- Enlarging/Reducing video window
- Low/High Bandwidth mode
- Snapshots
- Digital Zoom

Right-click on the video Window to get video streaming parameters such as actual frame rate and dimensions (resolution) of the image.

6.3.2.1 Single Playback Controls

You can use the Single Playback Control buttons in order to make the viewing process more flexible and controllable. The following **Single Playback Control** buttons are available:

- **Stop button** – stops playback and returns the slider to its initial position.
- **Frame Backward** – allows you to view the recording in the 'frame-by-frame' mode in reverse direction.
- **Play/Pause** – start or pause the playback. After you press this button the slider is not automatically returned to its initial position.
- **Fast Forward** – increase the playback speed in order to skip the irrelevant information. You can choose from 2x, 4x or 8x speed by clicking on the button.
- **Frame Forward** – allows you to view the recording in the "frame-by-frame" mode.

6.3.2.2 Switching sources

You can switch between all cameras available on your system by clicking the corresponding camera buttons. By doing this, you will get the recording from that camera for the selected time period. Note that the slider position remains the same while switching between cameras.

6.3.2.3 Activity Level

The **Activity level** for the specified time period is displayed below the video for ease of use. When there is no green activity line drawn or if the green activity line is drawn below the red activity threshold line, no recorded video footage exists for these periods.

6.3.2.4 Slider

Use the **slider** to quickly look through the recording.

6.3.2.5 Changing Video Window Size

You can change the size of the window in which the camera stream is visualized.

Click the button in order to make the Video Window **smaller**.

Click the button in order to make the Video Window **bigger**.

6.3.2.6 Low/High Bandwidth Mode

Low/High bandwidth mode allows you to decide if you want to have streaming video that consumes a reduced bandwidth. You can choose between:

- **High Bandwidth Mode** (Default) – High Bandwidth mode is used preferably on local computers (when the WebCCTV client is located on the same machine as the WebCCTV server), in local area networks or with high-speed Internet connections. Use the **High** ( ) button to enable high bandwidth mode.

- **Low Bandwidth Mode** – Low bandwidth mode is mostly used in medium- or slow-speed LAN or Internet connections. When Low Bandwidth mode is enabled, the frame rate and the resolution of the images are reduced. This leads to a reduced bandwidth usage for streaming. Use the **Low** (

) button to enable low bandwidth mode.

6.3.2.7 Snapshots

This WebCCTV feature gives you the opportunity to make snapshots. To create a snapshot, follow the steps below:

1. Choose the frame you want to save and click the button with the camera symbol ( ).
2. Choose the desired location for storing images and click the **Save** button.

Snapshots are saved in .JPEG format.

6.3.2.8 Digital Zoom

The Digital Zoom functionality is very useful when there are small details in the scene, but the camera doesn't support optical zoom and there's no way to visually enlarge those objects.

In order to use the Digital Zoom functionality, follow the steps below:

1. Click on the Video Window in order to set a focus point.
2. Use the mouse wheel to zoom the image in and out (a magnifying glass is shown).
3. When partially or totally zoomed in, click on any point of the video screen in order to centralize the video window on this point. This also resets the focus point for additional zooming in and out.

You cannot use the Digital Zoom functionality if your mouse doesn't have a mouse wheel.

6.3.3 Synchronized Playback

This feature allows you to view recorded footage simultaneously for up to four cameras. Playback from all four cameras is synchronized in time. The synchronized playback feature allows viewing the recorded video depending exclusively on time and not on video presence, i.e. it doesn't jump over the time spans without recordings.

To do a synchronized playback, follow the steps below:

1. Select the time period (see ***4.3.1 Select Time Period***).
2. Check the **Synchronized playback** radio button.
3. Choose **four cameras** from the drop-down lists.
4. Click the **Search** button.
5. For a new synchronized playback recording search, click the **New Search** button.

Recordings Synchronized Playback Screen

When you have the recording mode open, the following functionalities are available:

- Synchronized playback controls
- Switching sources
- Slider
- Enlarging/Reducing video window

Double click on the video window of a camera in order to switch to single playback of this camera.

The **Snapshots, High/Low Bandwidth**, **Digital Zoom** and **Activity level** functionalities are not available in synchronized playback.

6.3.3.1 Synchronized Playback Controls

You can use the Synchronize Playback Control buttons in order to make the viewing process more flexible and controllable. The following **Synchronized Playback Control** buttons are available:

- **Stop button** – stops playback and returns the slider to its initial position.
- **Frame Backward** – allows you to view the recording in the 'frame-by-frame' mode in reverse direction.
- **Play/Pause** – start or pause the playback. After you press this button the slider is not automatically returned to its initial position.
- **Frame Forward** – allows you to view the recording in the "frame-by-frame" mode.

6.3.3.2 Switching sources

You can switch between all available cameras for every video window by selecting the camera from the drop-down list. By doing this, you will get the recording from that camera for the same time period. Note that the slider position remains the same while switching between cameras and that the slider has the same position synchronized in time for all four cameras.

6.3.3.3 Slider

Use the **slider** to quickly look through the recording.

6.3.3.4 Changing Video Window Size

You can change the size of the window in which the camera stream is visualized.

Click the button in order to make the Video Window **smaller**.

Click the button in order to make the Video Window **bigger**.

6.3.4 Alarms

WebCCTV allows searching specifically for recordings from cameras associated with certain alarms. In order to search for alarms recordings, follow the steps below:

1. Select the time period (see ***6.3.1 Select Time Period***).
2. Check the **Alarm listing** radio button.
3. Choose the **alarm** from the drop-down list.
4. Click the **Search** button.
5. For a new alarm recording search, click the **New Search** button.

Recording Alarms Screen

Click on the camera buttons or event links to see the recordings associated with the alarm events.

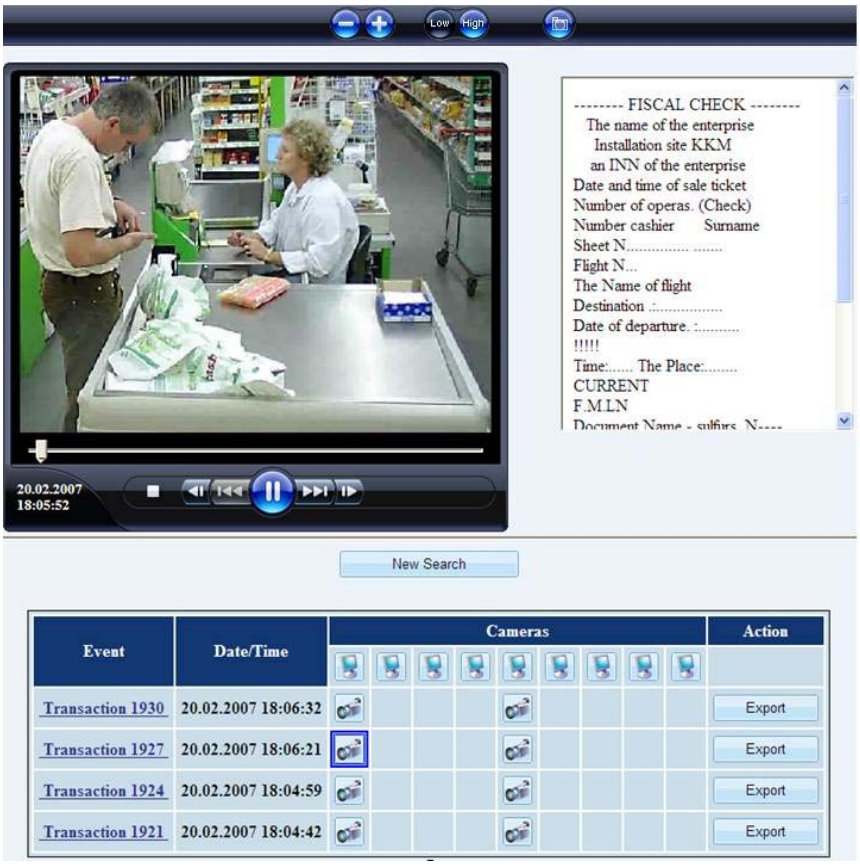
When you have the recording alarms screen open, this is identical to the one in the Alarms menu. The only difference is that you only have the alarms for the time period you requested.

For more explanation about all the functionalities you can use in this screen, see **6.*4 Alarms***.

6.3.5 POS

WebCCTV allows searching specifically for recordings from cameras associated with certain POS transactions. In order to search for POS transaction recordings, follow the steps below:

1. Select the time period (see ***6.3.1 Select Time Period***).
2. Check the **POS** radio button.
3. Check a radio button out of the following three options:
    a. **POS** – select the POS source from the drop-down list.
    b. **Transaction ID** – fill in the ID of the transaction you wish to see.
    c. **Transaction data** – fill in some data (e.g. cola) in order to get all transactions where that word is included.
4. Click the **Search** button.
5. For a new POS transaction recordings search, click the **New Search** button.



Recordings POS Screen

Click on the camera buttons or event links to see the recordings associated with the transactions.

When you have the recording POS screen open, this is identical to the one in the POS menu. The only difference is that you only have the alarms for the time period you requested.

For a more detailed explanation about all the functionalities you can use in this screen, see **6.*5 Alarms***.

6.3.6 Movie Export

This chapter provides an overview of the export capabilities of WebCCTV and covers the following topics:

- Creating movie export files.
- Saving movie export files on your computer.
- Saving movie export files to a CD / DVD disk.
- Checking the digital signature of movie export files.

Recordings Export Screen

6.3.6.1 Creating Export

To create a movie export file, follow the steps below:

1. Select the time period (see ***4.3.1 Select Time Period***).
2. Check the **Movie export** radio button.
3. Choose the **camera** from the drop-down list.
4. Click the **Search** button.

The specified time period should be within 1 minute to 1 hour range.

6.3.6.2 Saving Export Files to Hard Disk

After you clicked the **Search** button, your **Export files** will become visible beneath the **Recordings screen**.

To save an export file on your local disk, please follow the steps below:

1. **Right click** on the export file you want to save.
2. From the pop-up menu that appears, choose **Save Target As…**

Recordings Export Screen

3. Define the destination and click the **Save** button.

To delete the export files, select the export files you want to delete and click the **Delete** button**.**

The Compression format (JPEG, MPEG) for recordings is defined in the Camera wizard during the camera set-up in the Video Manager application.

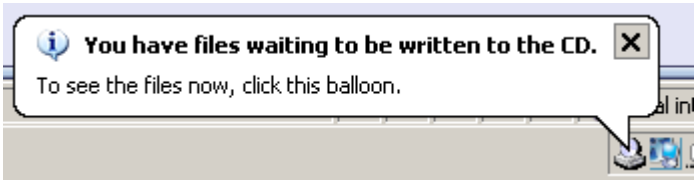
6.3.6.3 Saving Export Files to CD

To save an exported movie file to the CD follow the steps below:

1. **Right click** on the export file you want to save.
2. From the pop-up menu that appears choose **Save Target As…**

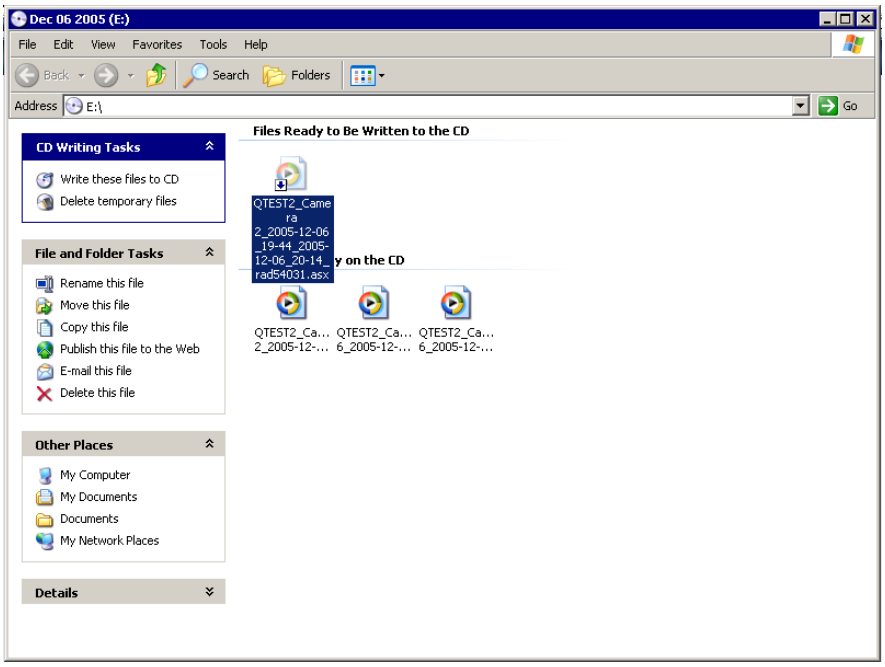
Recordings Export Screen

3. Choose your CD-RW drive as destination and click **Save**.
4. Wait until downloading is complete and click **Close**. At the bottom of your screen a message in your tray appears:



5. Click on the message. In the window that appears, select the shortcut to the file you want to save under the **Files Ready to Be Written to the CD** title.

This can also be done in File Explorer if the event notifications are disabled.



CD Explorer Screen

6. Click **Write this file to CD** in the left pane of the screen. The **CD Writing Wizard** screen appears.

CD Writing Wizard
Welcome to the CD Writing Wizard
This wizard helps you write, or record, your files to a CD recording drive.
Type the name you want to give to this CD, or just click Next to use the name below.
CD name:
Movies
New files being written to the CD will replace any files already on the CD if they have the same name.
Close the wizard after the files have been written
< Back
Next >
Cancel

CD Writing Wizard Screen

7. To begin the writing process, click the **Next** button.
8. After the writing process is complete, click the **Finish** button to close the CD Writing Wizard.

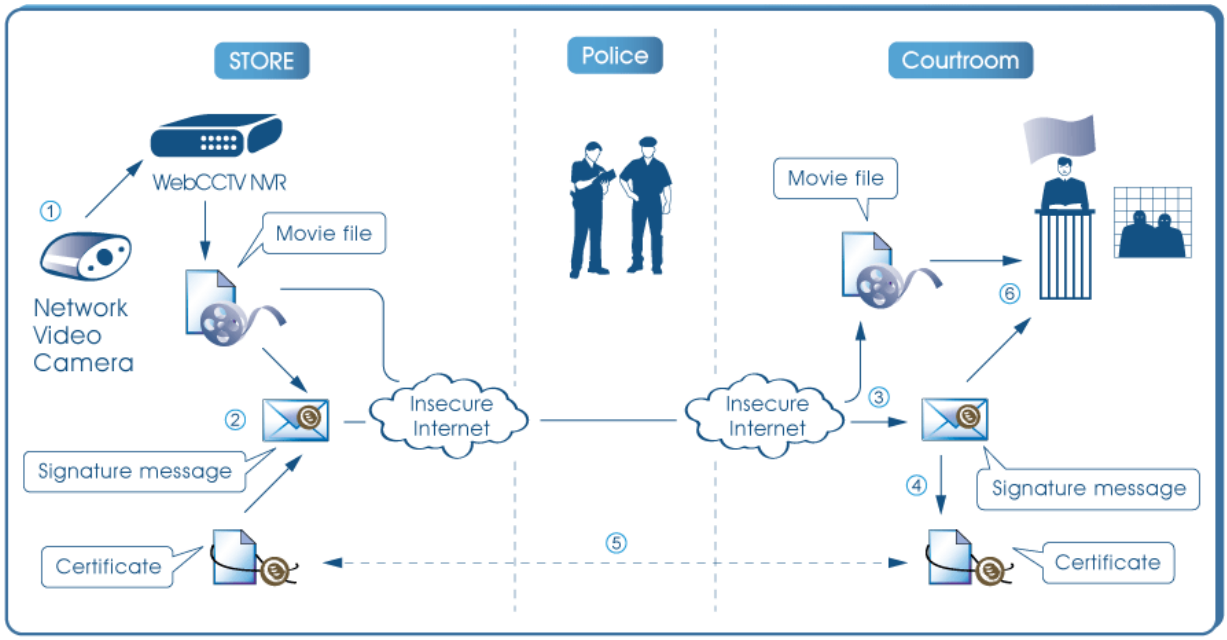
6.3.6.4 Checking Digital Signature

The latest generation of networked systems promises a much easier and faster way of moving video around (e.g. police, court room…), by simply sending it over the Internet. A public network like the Internet is not exactly the safest when talking about transport. However, digital video can be digitally secured and the possibility to trace the video back to its origin is now a reality. This technology is called **digitally signing** the video.

A **digital signature** is a cryptographically encoded text that contains information about the exported movie file that was signed and about the entity that created the signature. Each export file has its own signature.

A **certificate** is again a cryptographically protected text that contains the electronic key with which the owner of the certificate can sign digital documents or content. This certificate is only valuable if it is trusted by the authorities.

The following diagram shows how a digital signature is used in the video authentication process:



Video Authentication Process

Step 1 - Recording

Video from the camera is recorded in a standard ASF movie file.

Step 2 - Export

When a relevant piece of video is exported, information about that video (e.g. the timestamp, camera name, recorder information and the user who performed the export) is gathered in a signature message. This message is encrypted by the certificate, unique to each recorder, to form a digital signature.

WebCCTV supports two formats of digital signatures:

- **.eml** – S/MIME standard message like used in digitally signed emails.
- **.p7m** – true PKCS #7 standard signature message. It can be opened by specialized viewers like Cryptigo's P7MViewer (http://www.cryptigo.com).

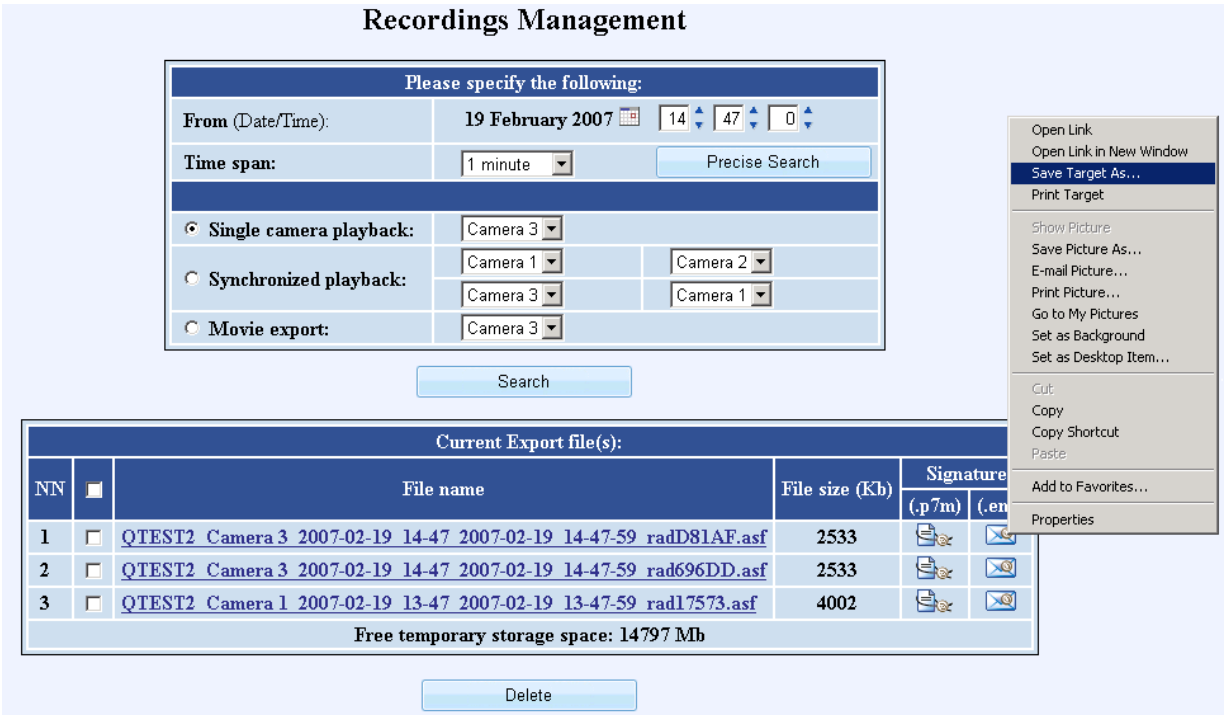
Quadrox has based all of these systems on the open standard technology to prevent any possibility of security holes or "back doors". All algorithms that are used are well known and widely used cryptographic standards, like MD5, SHA-1 and RSA. They cannot be broken if the key is not known, not even by the people that implemented them. The certificate is standard (X.509, PKSC #12), as is the digital signature format (PKCS #7). Apart from the true signature standard that can be viewed by publicly available specialized viewers, we also provide the signature in a standard email format (S/MIME format) so that it can be viewed by common email clients like Outlook Express. Quadrox uses Microsoft's implementations of these formats and algorithms, which are validated and certified by the National Institute of Standards and Technology (NIST).

Step 3 – Signature and movie transportation

The movie file and the signature are transported to the courtroom. They don't necessarily have to travel together and the channel can be unsafe (e.g. they can be sent over the Internet).

To save the signature for further transportation, follow the steps below:

1. Right click on the signature you want to save.
2. From the pop-up menu that appears choose **Save Target As…** and define the destination.



Saving Digital Signature Screen

Step 4 + Step 5 - Certificate transportation and trust

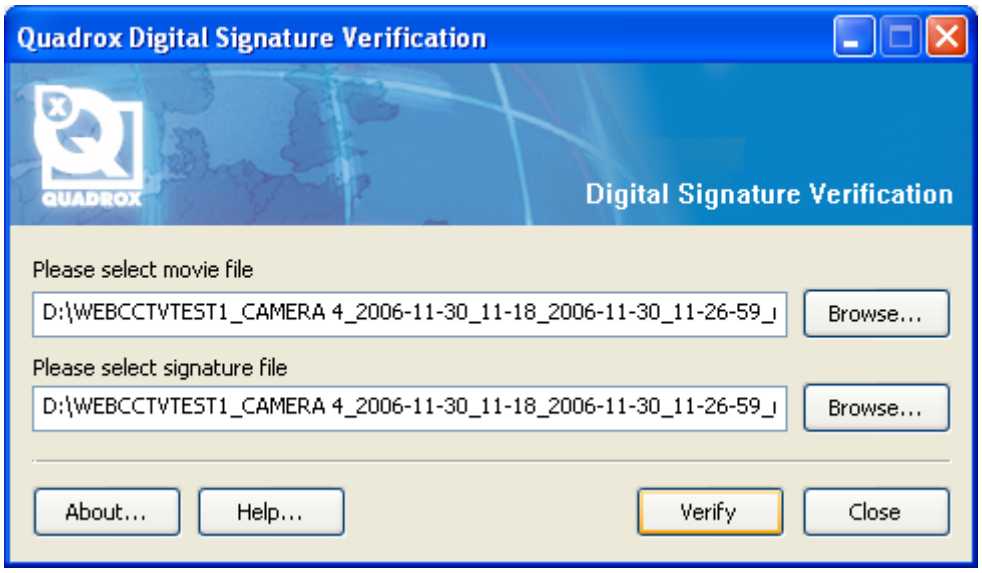
The certificate should be trusted by the court. By trusting the validity of a certificate (by manually checking that it is indeed what it claims to be), the court acknowledges explicitly that the certificate belongs to the machine on which the export was created.

The court expresses this trust by explicitly adding it to the list of trusted root certificates. When doing this, the system will ask to manually verify the certificate, e.g. by comparing the thumbprint of the certificate to the thumbprint of the certificate that is present on the recorder. The latter should be retrieved by physically going to the recorder, it should be done by the authorities and a proven track record should be available. Trusting the certificate has to be done only once per recorder (not for every movie) and doesn't necessarily have to happen at the moment of movie verification.

When using CA certificates, the trust in the certificate might come from trusting the CA that delivered the certificate. In that case, this procedure might not be necessary.

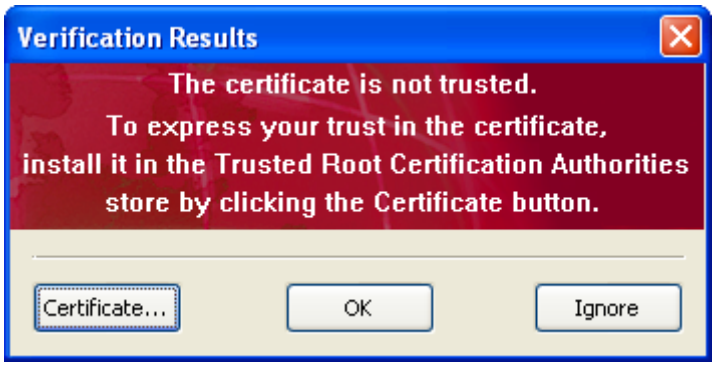
A copy of the certificate can be extracted from the signature by using the Digital Signature Verifier (available from the Quadrox website). The certificate can also get to the courtroom in a different way (by exporting it from the recorder) or can already be present because it was extracted from previous movies.

To extract and install the certificate from the signature itself using the Digital Signature Verifier, follow the steps below:



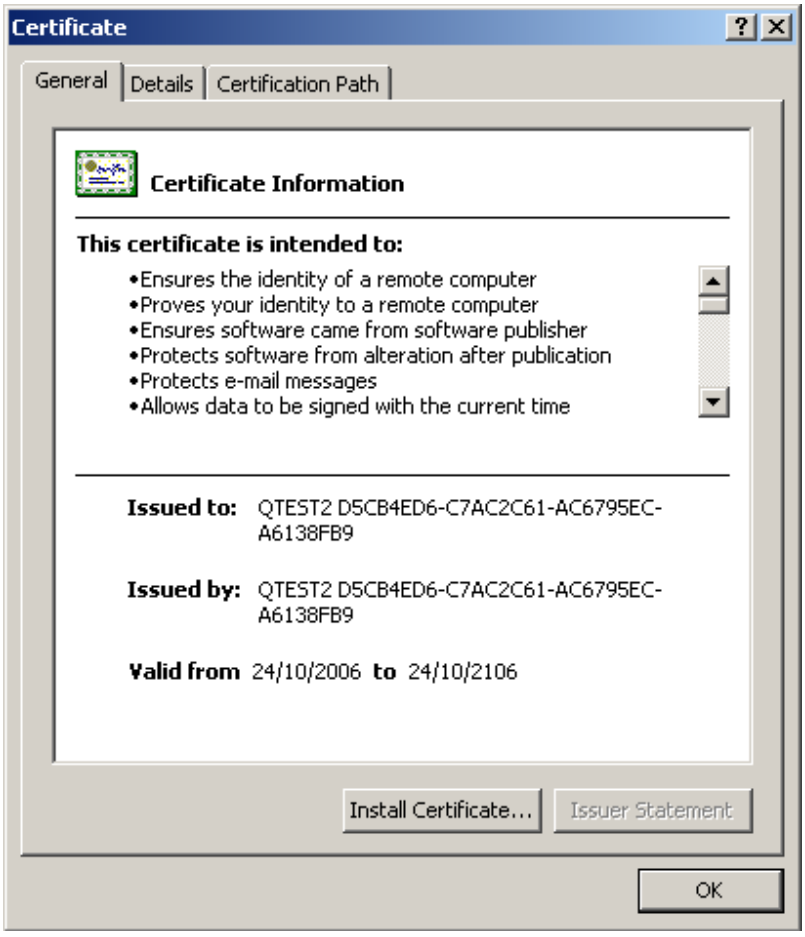
Digital Signature Verifier main screen

1. Open the Digital Signature Verifier tool.
2. Enter the locations of the movie and signature files and click the **Verify** button. If the certificate is not yet trusted, you will see the following screen.


Verification Results
The certificate is not trusted.
To express your trust in the certificate, install it in the Trusted Root Certification Authorities store by clicking the Certificate button.
Certificate...
OK
Ignore

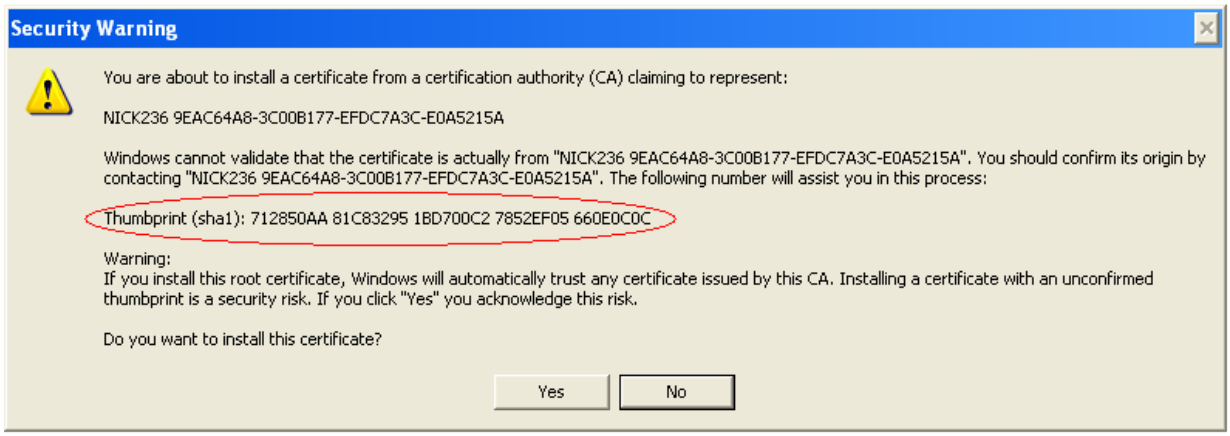
Not trusted certificate warning screen

3. Click the **Certificate** button.

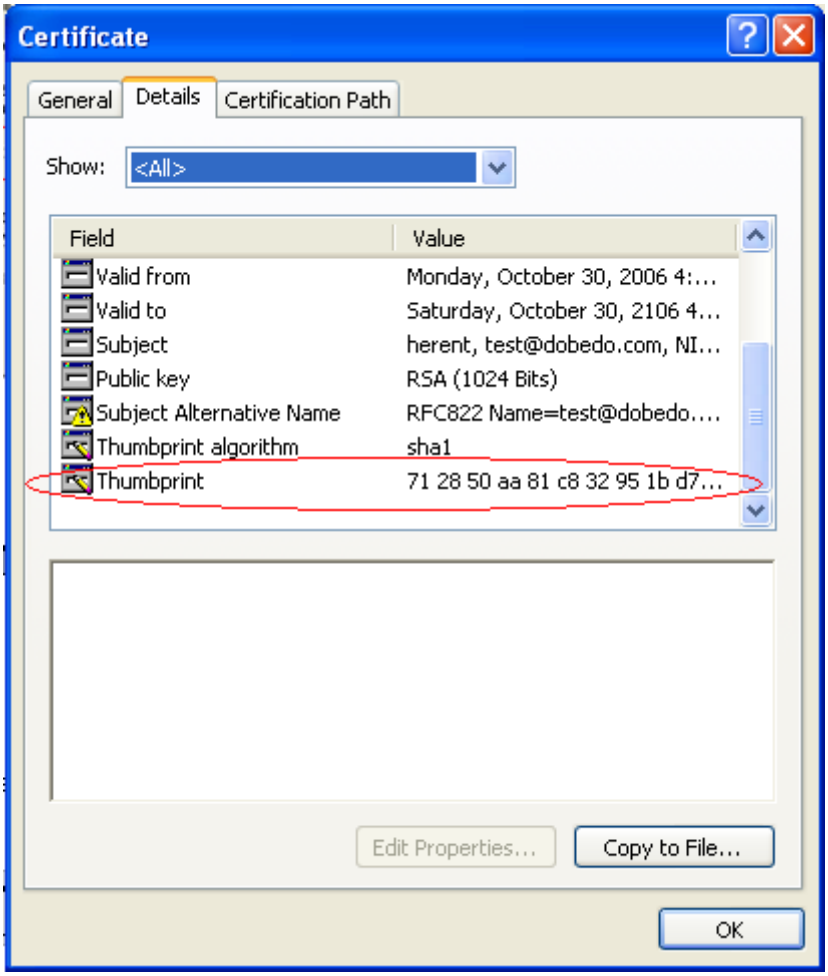


Certificate Information Screen

4. Click the **Install Certificate** button and follow further instructions leaving all settings by default. A Security Warning window will appear.
5. To make sure that you are installing the exact certificate you need, find the **Thumbprint** line in the Security Warning window and compare it with the thumbprint of the original certificate on the recorder. If the thumbprints match, click **Yes**.


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
NICK236 9EAC64A8-3C00B177-EFDC7A3C-E0A5215A
Windows cannot validate that the certificate is actually from "NICK236 9EAC64A8-3C00B177-EFDC7A3C-E0A5215A". You should confirm its origin by contacting "NICK236 9EAC64A8-3C00B177-EFDC7A3C-E0A5215A". The following number will assist you in this process:
Thumbprint (sha1): 712850AA 81C83295 1BD700C2 7852EF05 660E0C0C
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

Security Warning Screen

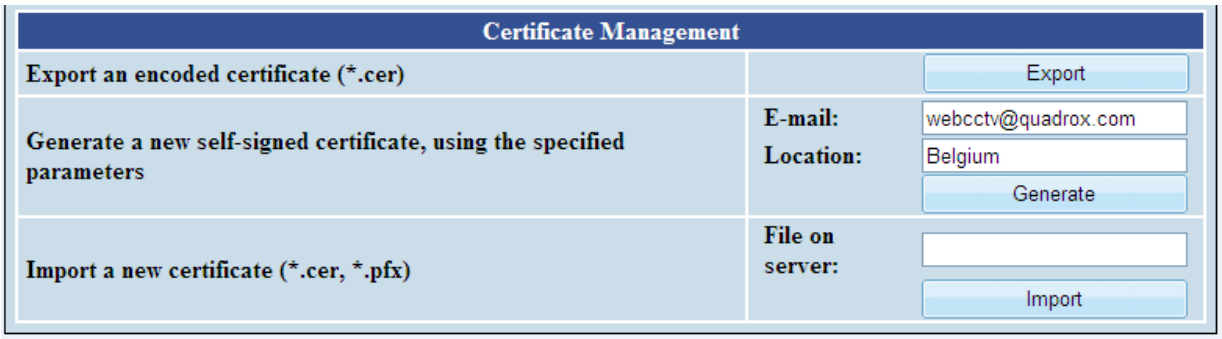


Certificate Information Screen

6. Once your certificate is installed, repeat step 2 to verify the signature. See also "Step 6 – Checking the signature" below.

To install the certificate by exporting it from the recorder, follow the steps below:

1. Open WebCCTV web-client.
2. Go to **System-> Certificate Management** section.
3. Click **Export** button and define location to store the certificate.



Certificate Management Screen

4. Transport the exported certificate to the target machine and double click on it. The Certificate Information screen will appear.
5. Click the **Install Certificate** button and follow further instructions leaving all settings by default. A Security Warning window will appear.
6. To make sure that you are installing the exact certificate you need, find the **Thumbprint** line in the Security Warning window and compare it with the thumbprint of the original certificate on the recorder. If the thumbprints match, click **Yes**.

To learn advanced ways to make the certificate explicitly trusted, see **Appendix A**.

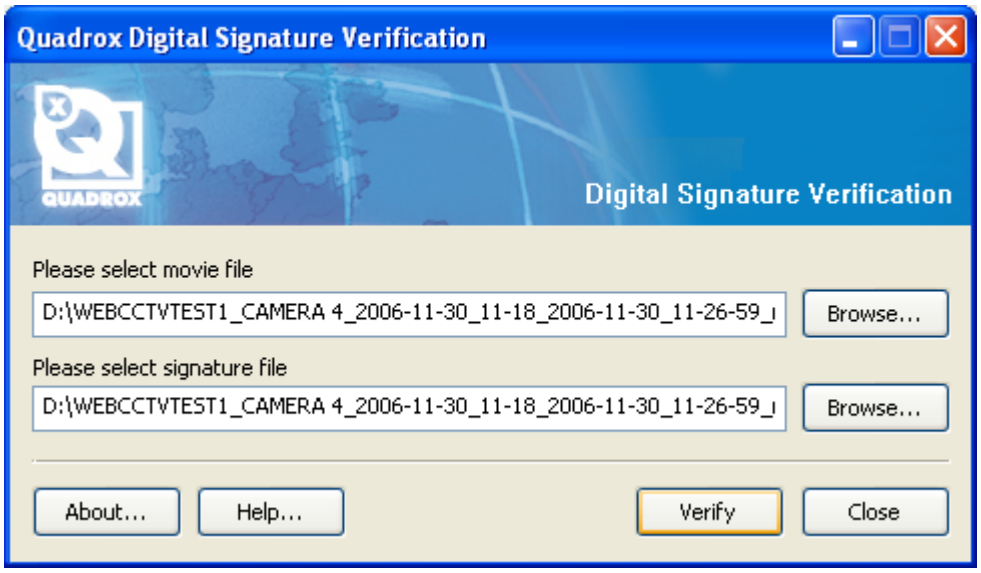
Step 6 – Checking the signature

Once the certificate is trusted, the signature message can be decoded. Because the certificate is trusted, we know that
a) the information in the signature is correct (wasn't changed) and
b) the signature was produced on the recorder from which the movie is claimed to have originated. If the signature was forged, the certificate will not decode it.

Inside the signature, a hash value links the certificate uniquely to the movie file. By recalculating the hash in the courtroom, we can be sure that
a) this signature belongs to this particular movie and
b) the movie hasn't changed since the signature was created.

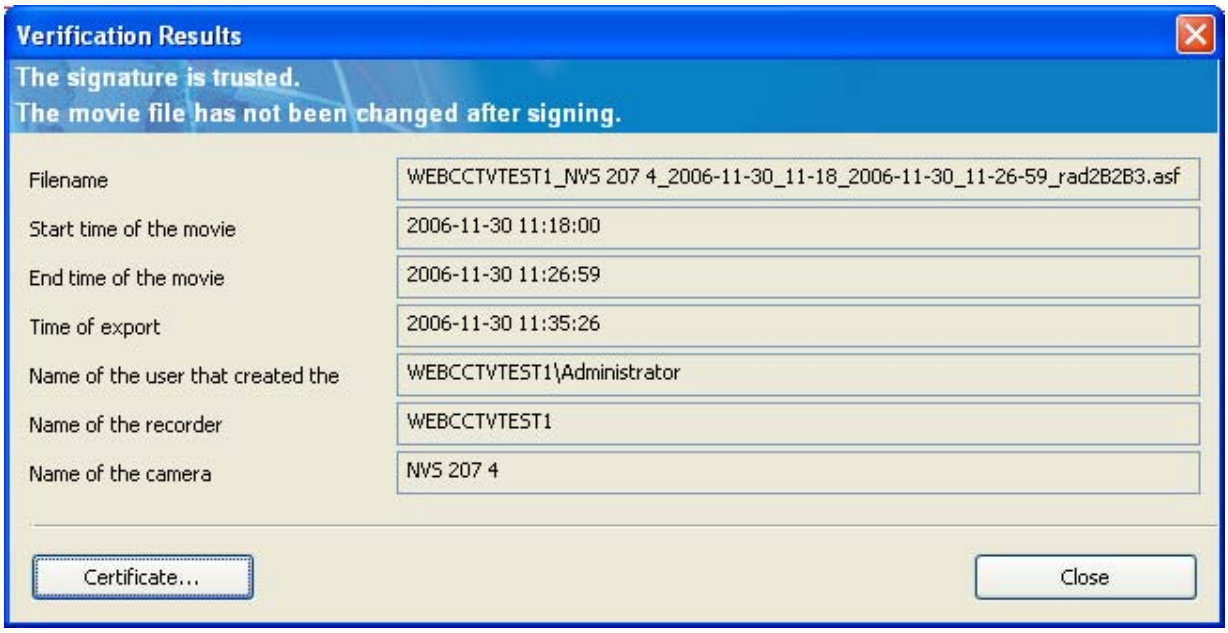
If the movie was forged, the hash value would be different and the signature invalid.

These actions are performed automatically by the Digital Signature Verifier tool.



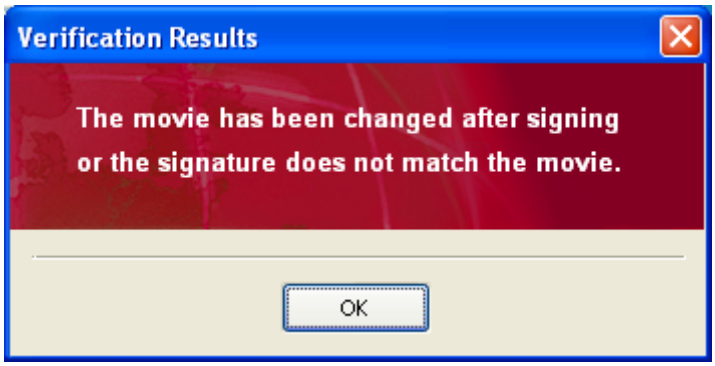
Digital Signature Verifier main screen

1. Open the Digital Signature Verifier tool.
2. Enter the locations of the movie and signature files and click the **Verify** button.
3. If the signature can be decoded and the hash information matches the movie, the movie authenticity is proven and the following information screen will be shown. The displayed information is part of the digital signature and is likewise proven to be authentic.



Trusted signature information screen

4. If the signature cannot be trusted because either the signature or the movie was tampered with, the following screen will be shown.



Not trusted signature information screen

The Digital Signature Verifier was created by Quadrox to make your life easier. However, it is not crucial to verify the digital signature. You are free to manually check the signature, or by a tool of your own choice.

The tool is released as an open source tool under the BSD license. To make sure that the tool doesn't display false information, feel free to examine the source code and make your own compilation for maximum trust.

To learn how to manually verify the signature, see **Appendix B**.

6.4 Alarms

The **Alarms Menu** allows you to view and export recorded alarm events generated on incoming alarms.

The **Alarm Component** has to be installed to see the menu.

The following sections are described:

- View alarm movie
- Export alarm movie
- Slider
- Alarm playback controls
- Enlarging/Reducing video window
- Low/High Bandwidth mode
- Snapshots
- Digital Zoom

Alarms Screen

6.4.1 View Alarm Movie

In the Alarm Screen, you get a list of all the alarms with their associated recordings. Furthermore you also get the **date** and **time** of each alarm event.

Each new incoming active alarm is highlighted in **red**. To view the alarm movie, click on the **alarm event link** and the movie of the first added camera will be displayed in the video window screen. When the alarm link is clicked, the alarm is deactivated and loses its red color. You can switch between all cameras that are associated with an alarm event by clicking the corresponding camera icon . If you want to see the live view of the cameras, click on the following icons.

The list is limited to the 5 most recent deactivated alarm events if all are in deactivated state. Activated alarms stay visible until deactivated, up to a maximum of 50.

Click the **Deactivate All** button if you want to deactivate all alarms.

When clicking on the alarm name, the recording of the first camera connected to that alarm is shown. If no recordings are connected to that alarm, you will see the live view from the camera that is first in the camera list.

To extend the alarm pane, click on its upper board and move it to the top of the screen while holding the left mouse button.

A new alarm is called active and has a red color . A previously viewed alarm is called de-activated and is shown in blue.

If you don't see your alarm event in the list, you can search it by clicking the **New Search** button which will redirect you to the recordings menu (see **6.*3.4 Alarms***).

6.4.2 Export Alarm Movie

You can export alarm movies as .asf files while staying on the **Alarms** page. In order to export the alarm movie, click the **Export** button of the alarm event and wait while WebCCTV creates an export movie for each associated active camera(s) in the **Recordings Menu**.

6.4.3 Slider

Use the **slider** to quickly look through the recording.

6.4.4 Alarm Playback Controls

You can use the Alarm Playback Control buttons in order to make the viewing process more flexible and controllable. The following **Alarm Playback Control** buttons are available:

- **Stop button** – stops the playback and returns the slider to its initial position.
- **Frame Backward** – allows you to view the recording in the 'frame-by-frame' mode in reverse direction.
- **Play/Pause** – starts or pauses the playback. After you press this button the slider is not automatically returned to its initial position.
- **Fast Forward** – increase the playback speed in order to skip the irrelevant information. You can choose from 2x, 4x or 8x speed by clicking on the button.
- **Frame Forward** – allows you to view the recording in the "frame-by-frame" mode.

6.4.5 Changing Video Window Size

You can change the size of the window in which the camera stream is visualized.

Click the button in order to make the Video Window **smaller**.

Click the button in order to make the Video Window **bigger**.

6.4.6 Low/High Bandwidth Mode

Low/High bandwidth mode allows you to decide if you want to have streaming video that consumes a reduced bandwidth. You can choose from:

- **High Bandwidth Mode** (Default) – High Bandwidth mode is used preferably on local computers (when the WebCCTV client is located on the same machine as the WebCCTV server), in local area networks or with high-speed Internet connections. Use the **High** ( ) button to enable the high bandwidth mode.
- **Low Bandwidth Mode** – Low bandwidth mode is mostly used in medium- or slow-speed LAN or Internet connections. When Low Bandwidth mode is enabled, the frame rate and the resolution of the images are reduced. This produces reduced bandwidth usage for streaming video. Use the **Low** ( ) button to enable the low bandwidth mode.

6.4.7 Snapshots

This WebCCTV feature gives you the ability to take snapshots. To create a snapshot, follow the steps below:

1. Choose the frame you want to save and click the button with the camera symbol ( ).
2. Choose the desired location for storing images and click the **Save** button.

Snapshots are saved in .JPEG format.

6.4.8 Digital Zoom

The Digital Zoom functionality is very useful when there are small details in the scene but the camera doesn't support optical zoom and there's no way to visually enlarge those objects.

In order to use the **Digital Zoom** functionality, follow the steps below:

1. Click on the video window in order to set a focus point.
2. Use the scroll wheel to zoom the image in and out (a magnifying glass is shown).
3. When partially or totally zoomed in, click on any point of the video screen in order to centralize the video window on this point. This also resets the focus point of further zooming in and out.

You cannot use the Digital Zoom functionality if your mouse doesn't have a scroll wheel.

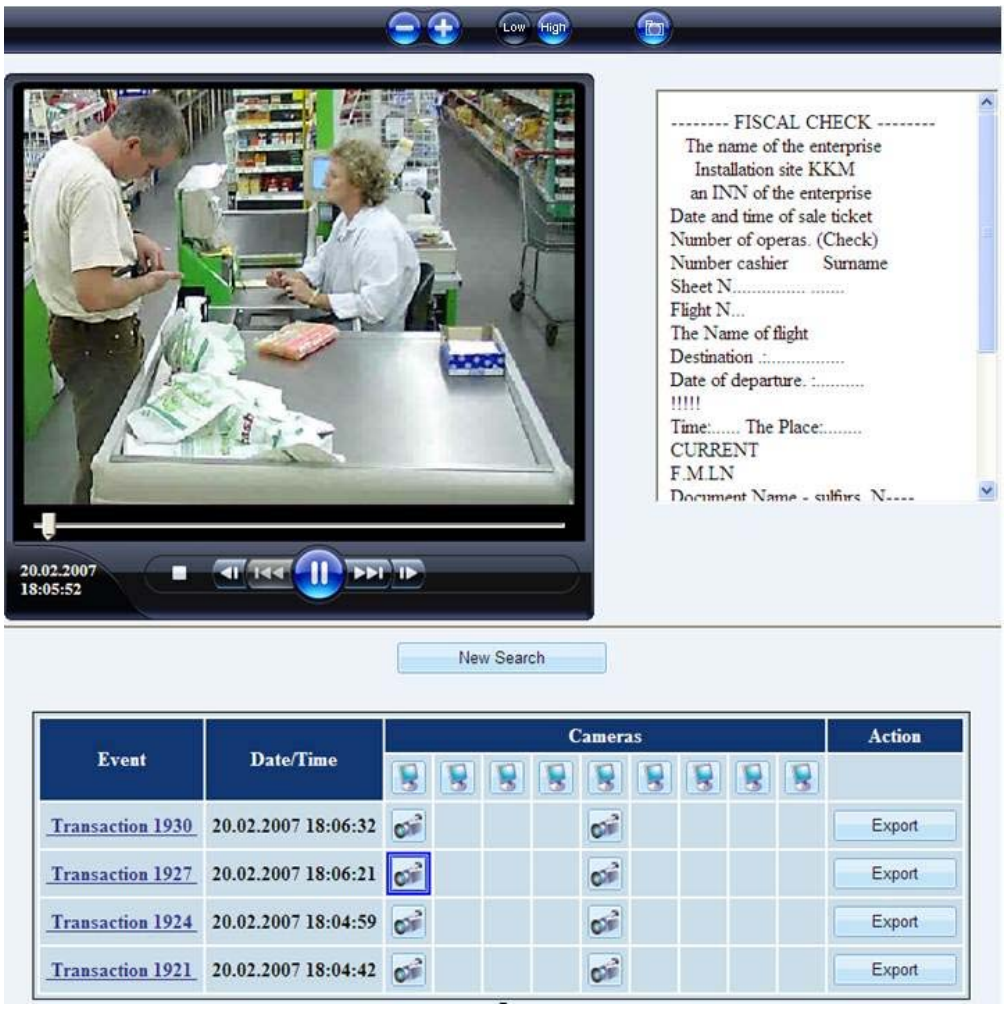
6.5 POS

The **POS Menu** allows you to view recorded POS transaction movies and tickets and export the associated POS transaction movies.

The **Alarm Component** has to be installed to see the menu.

The following sections are described:

- View POS movie and ticket
- Export POS movie
- Slider
- POS playback controls
- Enlarging/Reducing video window
- Low/High Bandwidth mode
- Snapshots
- Digital Zoom



POS Screen

6.5.1 View POS Movie and Ticket

In the POS Screen, you get a list of all the transactions with their associated recordings and tickets. Furthermore you also get the **date** and **time** of each POS transaction.

To view a POS transaction movie, click on the **transaction event link** and the movie of the first added camera will be displayed in the video window screen. You can switch between all cameras that are associated with a transaction by clicking the corresponding camera icon .

If you want to see the live view of the cameras, click on the following icons.

The list is limited to the 5 most recent deactivated alarm events if all are in deactivated state. Activated alarms stay visible until deactivated, up to a maximum of 50.

When clicking on the transaction name, the recording of the first camera connected to that transaction is shown. If no recordings are connected to that transaction, you will see the live view from the camera that is first in the camera list.

To extend the POS pane, click on its upper board and move it to the top of the screen holding the left mouse button.

If you don't see your transaction event in the list, you can search it by clicking the **New Search** button which will redirect you to the recordings menu (see **6.*3.5 POS***).

6.5.2 Export POS Movie

You can export POS transactions movies to .asf files while staying on the **POS** page. In order to export the POS movie, click the **Export** button of the POS transaction event and wait while WebCCTV creates an export movie for each associated camera(s) in the **Recordings Menu**.

6.5.3 Slider

Use the **slider** to quickly look through the recording.

6.5.4 POS Playback Controls

You can use the POS Playback Control buttons in order to make the viewing process more flexible and controllable. The following **POS Playback Control** buttons are available:

- **Stop button** – stops playback and returns the slider to its initial position.
- **Frame Backward** – allows you to view the recording in the 'frame-by-frame' mode in reverse direction.
- **Play/Pause** – start or pause the playback. After you press this button the slider is not automatically returned to its initial position.
- **Fast Forward** – increase the playback speed in order to skip the irrelevant information. You can choose from 2x, 4x or 8x speed by clicking on the button.
- **Frame Forward** – allows you to view the recording in the "frame-by-frame" mode.

6.5.5 Changing Video Window Size

You can change the size of the window in which the camera stream is visualized.

Click the button in order to make the Video Window **smaller**.

Click the button in order to make the Video Window **bigger**.

6.5.6 Low/High Bandwidth Mode

Low/High bandwidth mode allows you to decide if you want to have streaming video that consumes. You can choose from:

- **High Bandwidth Mode** (Default) – High Bandwidth mode is used preferably on local computers (when the WebCCTV client is located on the same machine as the WebCCTV server), in local area networks or with high-speed Internet connections. Use the **High** ( ) button to enable the high bandwidth mode.
- **Low Bandwidth Mode** – Low bandwidth mode is mostly used in medium- or slow-speed LAN or Internet connections. When Low Bandwidth mode is enabled, the frame rate and the resolution of the images are reduced. This produces a reduced bandwidth usage for streaming video. Use the **Low** ( ) button to enable the low bandwidth mode.

6.5.7 Snapshots

This WebCCTV feature gives you the opportunity to take snapshots. To create a snapshot, follow the steps below:

1. Choose the frame you want to save and click the button with the camera symbol ( ).
2. Choose the desired location for storing images and click the **Save** button.

Snapshots are saved in .JPEG format.

6.5.8 Digital Zoom

The Digital Zoom functionality is very useful when there are small details in the scene, but the camera doesn't support optical zoom and there's no way to visually enlarge those objects.

In order to use the **Digital Zoom** functionality, follow the steps below:

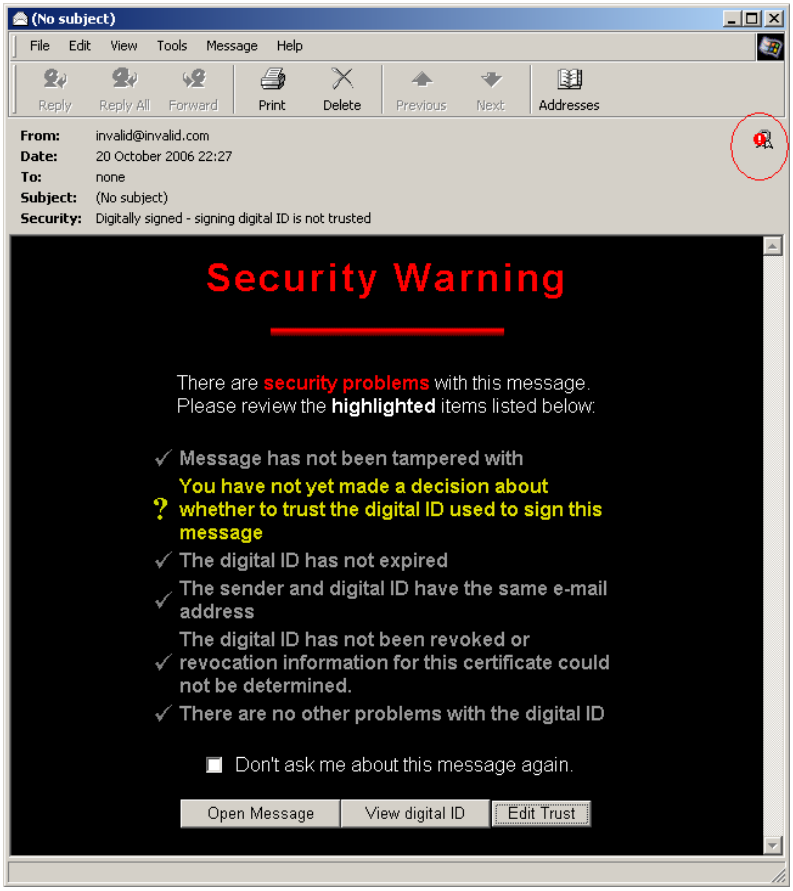
1. Click on the video window in order to set a focus point.
2. Use the scroll wheel to zoom the image in and out (a magnifying glass is shown).
3. When partially or totally zoomed in, click on any point of the video screen in order to centralize the video window on this point. This also resets the focus point of further zooming in and out.

You cannot use the Digital Zoom functionality if your mouse doesn't have a scroll wheel.

7 Appendix A

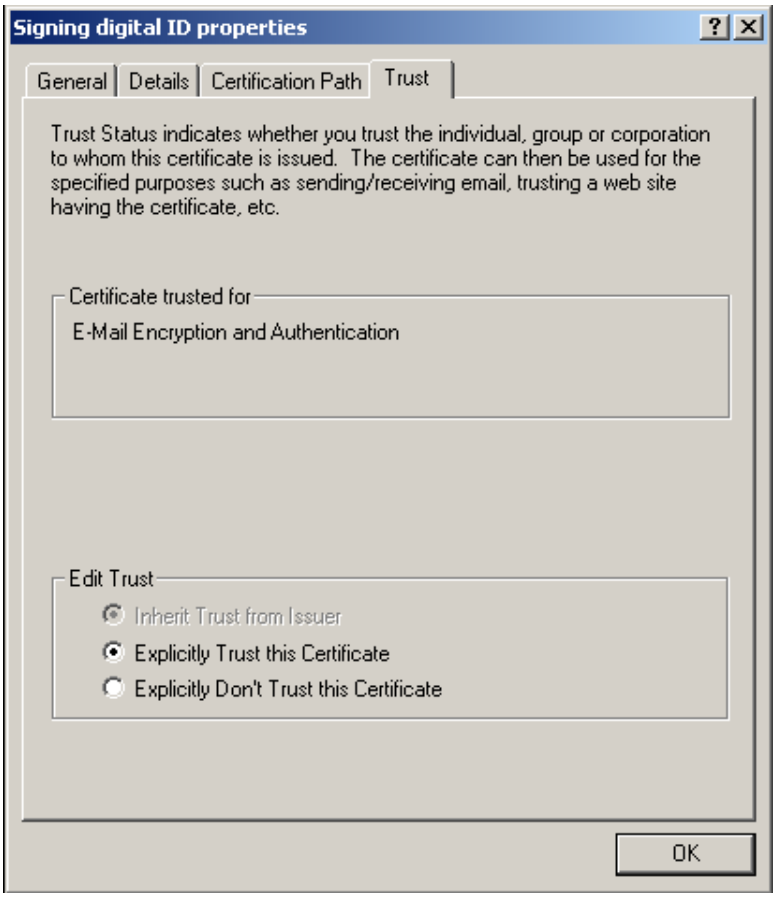
To make a certificate explicitly trusted by means of the Outlook Express email client, follow the steps below:

1. Save your **.eml** signature on the target machine.
2. Double-click on it to open. You will see the following screen that means your certificate is not trusted on this machine.


(No subject)
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: invalid@invalid.com
Date: 20 October 2006 22:27
To: none
Subject: (No subject)
Security: Digitally signed - signing digital ID is not trusted
Security Warning
There are security problems with this message.
Please review the highlighted items listed below:
Message has not been tampered with
You have not yet made a decision about whether to trust the digital ID used to sign this message
The digital ID has not expired
The sender and digital ID have the same e-mail address
The digital ID has not been revoked or revocation information for this certificate could not be determined.
There are no other problems with the digital ID
Don't ask me about this message again.
Open Message
View digital ID
Edit Trust

MS Outlook Express Untrusted Signature Screen

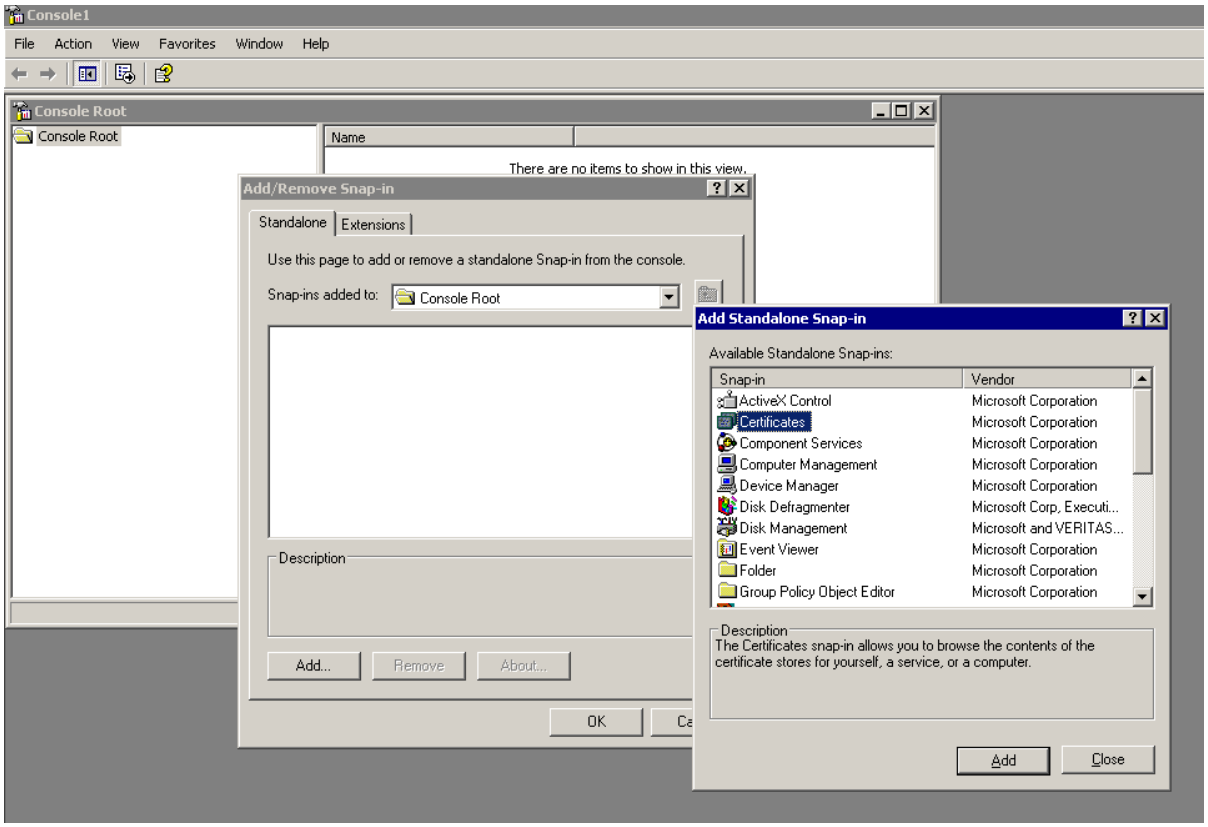
3. Click the **Edit Trust** button.
4. In the screen that appears select **Explicitly Trust this Certificate** and follow further prompts.


Signing digital ID properties
General
Details
Certification Path
Trust
Trust Status indicates whether you trust the individual, group or corporation to whom this certificate is issued. The certificate can then be used for the specified purposes such as sending/receiving email, trusting a web site having the certificate, etc.
Certificate trusted for
E-Mail Encryption and Authentication
Edit Trust
Inherit Trust from Issuer
Explicitly Trust this Certificate
Explicitly Don't Trust this Certificate
OK

Signing Digital ID Properties Screen

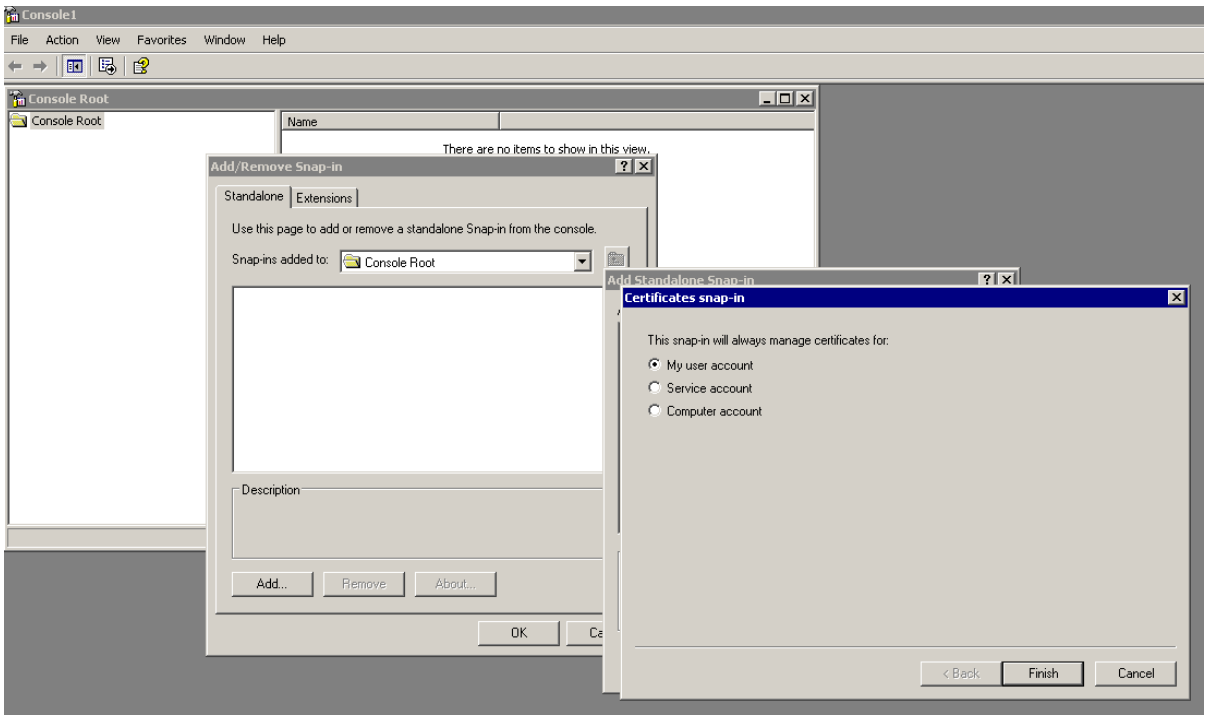
To make a certificate explicitly trusted by means of the Microsoft Management Console follow the steps below:

1. Go to **Start->Run** and specify the **mmc** command.
2. In the window that appears, click **File** in the window menu and select **Add/Remove Snap-in**.
3. In the window that appears, click the **Add** button.
4. In the next appeared window, choose **Certificates** and click the **Add** button.


Console1
File Action View Favorites Window Help
Console Root
Console Root
Name
There are no items to show in this view.
Add/Remove Snap-in
Standalone Extensions
Use this page to add or remove a standalone Snap-in from the console.
Snap-ins added to: Console Root
Description
Add... Remove About...
OK
Add Standalone Snap-in
Available Standalone Snap-ins:
Snap-in Vendor
ActiveX Control Microsoft Corporation
Certificates Microsoft Corporation
Component Services Microsoft Corporation
Computer Management Microsoft Corporation
Device Manager Microsoft Corporation
Disk Defragmenter Microsoft Corp, Executi...
Disk Management Microsoft and VERITAS...
Event Viewer Microsoft Corporation
Folder Microsoft Corporation
Group Policy Object Editor Microsoft Corporation
Description
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
Add Close

Microsoft Management Console Screen

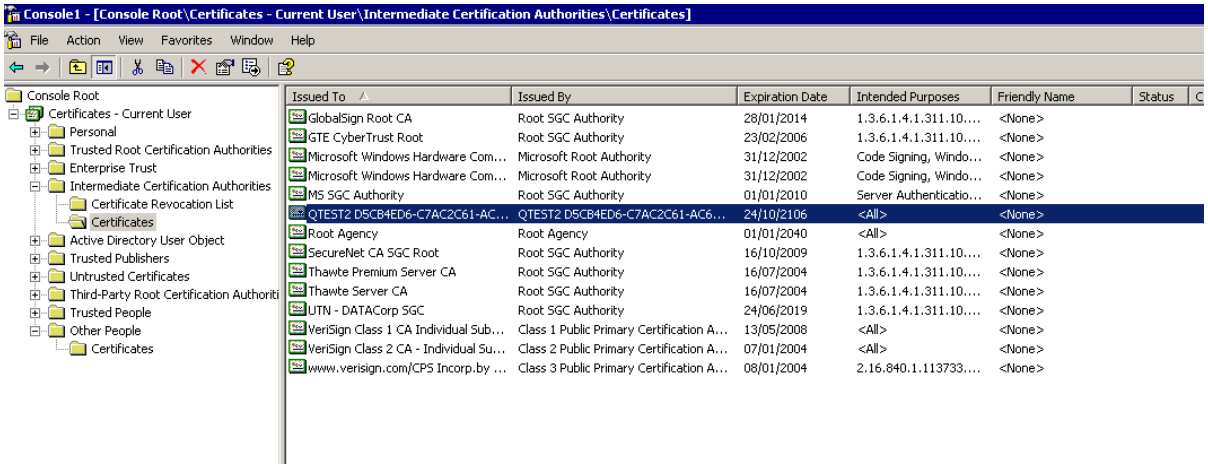
5. Then select **My User account** item and click **Finish**.



Microsoft Management Console Screen

6. Close all previously opened windows by pressing the **Close** and **OK** buttons.

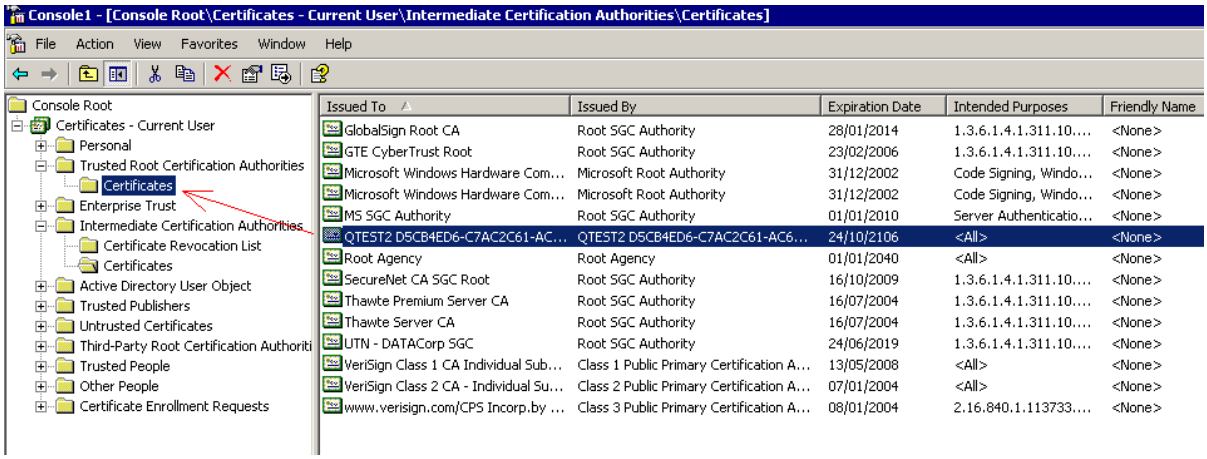
7. Finally you will get the list of all installed certificates.


Console1 - [Console Root\Certificates - Current User\Intermediate Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certificates
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Other People
Certificates
Issued To | Issued By | Expiration Date | Intended Purposes | Friendly Name | Status
GlobalSign Root CA | Root SGC Authority | 28/01/2014 | 1.3.6.1.4.1.311.10.... | <None>
GTE CyberTrust Root | Root SGC Authority | 23/02/2006 | 1.3.6.1.4.1.311.10.... | <None>
Microsoft Windows Hardware Com... | Microsoft Root Authority | 31/12/2002 | Code Signing, Windo... | <None>
Microsoft Windows Hardware Com... | Microsoft Root Authority | 31/12/2002 | Code Signing, Windo... | <None>
MS SGC Authority | Root SGC Authority | 01/01/2010 | Server Authenticatio... | <None>
QTEST2 D5CB4ED6-C7AC2C61-AC... | QTEST2 D5CB4ED6-C7AC2C61-AC6... | 24/10/2106 | <All> | <None>
Root Agency | Root Agency | 01/01/2040 | <All> | <None>
SecureNet CA SGC Root | Root SGC Authority | 16/10/2009 | 1.3.6.1.4.1.311.10.... | <None>
Thawte Premium Server CA | Root SGC Authority | 16/07/2004 | 1.3.6.1.4.1.311.10.... | <None>
Thawte Server CA | Root SGC Authority | 16/07/2004 | 1.3.6.1.4.1.311.10.... | <None>
UTN - DATACorp SGC | Root SGC Authority | 24/06/2019 | 1.3.6.1.4.1.311.10.... | <None>
VeriSign Class 1 CA Individual Sub... | Class 1 Public Primary Certification A... | 13/05/2008 | <All> | <None>
VeriSign Class 2 CA - Individual Su... | Class 2 Public Primary Certification A... | 07/01/2004 | <All> | <None>
www.verisign.com/CPS Incorp.by ... | Class 3 Public Primary Certification A... | 08/01/2004 | 2.16.840.1.113733.... | <None>

Microsoft Management Console Screen

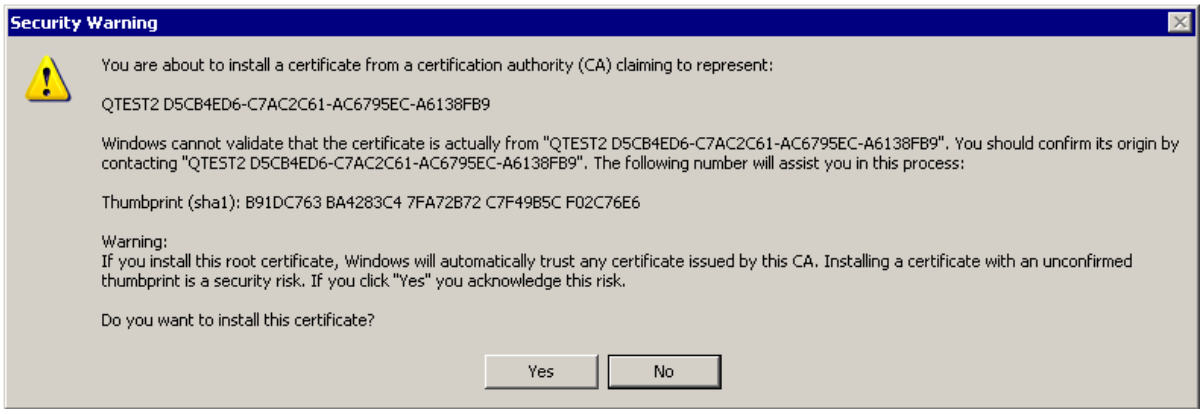
8. After the certificate installation procedures which were described above, the certificates are installed to the **Intermediate Certification Authorities** list (when a certificate is extracted from the digital signature) or to the **Other People** list (when a certificate is installed by exporting it from the recorder). Find your certificate in the corresponding list.

9. To make the certificate fully trusted, drag and drop your certificate to the **Trusted Root Certification Authorities** list.


Console1 - [Console Root\Certificates - Current User\Intermediate Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certificates
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Other People
Certificate Enrollment Requests
Issued To | Issued By | Expiration Date | Intended Purposes | Friendly Name
GlobalSign Root CA | Root SGC Authority | 28/01/2014 | 1.3.6.1.4.1.311.10.... | <None>
GTE CyberTrust Root | Root SGC Authority | 23/02/2006 | 1.3.6.1.4.1.311.10.... | <None>
Microsoft Windows Hardware Com... | Microsoft Root Authority | 31/12/2002 | Code Signing, Windo... | <None>
Microsoft Windows Hardware Com... | Microsoft Root Authority | 31/12/2002 | Code Signing, Windo... | <None>
MS SGC Authority | Root SGC Authority | 01/01/2010 | Server Authenticatio... | <None>
QTEST2 D5CB4ED6-C7AC2C61-AC... | QTEST2 D5CB4ED6-C7AC2C61-AC6... | 24/10/2106 | <All> | <None>
Root Agency | Root Agency | 01/01/2040 | <All> | <None>
SecureNet CA SGC Root | Root SGC Authority | 16/10/2009 | 1.3.6.1.4.1.311.10.... | <None>
Thawte Premium Server CA | Root SGC Authority | 16/07/2004 | 1.3.6.1.4.1.311.10.... | <None>
Thawte Server CA | Root SGC Authority | 16/07/2004 | 1.3.6.1.4.1.311.10.... | <None>
UTN - DATACorp SGC | Root SGC Authority | 24/06/2019 | 1.3.6.1.4.1.311.10.... | <None>
VeriSign Class 1 CA Individual Sub... | Class 1 Public Primary Certification A... | 13/05/2008 | <All> | <None>
VeriSign Class 2 CA - Individual Su... | Class 2 Public Primary Certification A... | 07/01/2004 | <All> | <None>
www.verisign.com/CPS Incorp.by ... | Class 3 Public Primary Certification A... | 08/01/2004 | 2.16.840.1.113733.... | <None>

Microsoft Management Console Screen

10. After verifying the thumbprint, click **Yes** in the screen that appears.

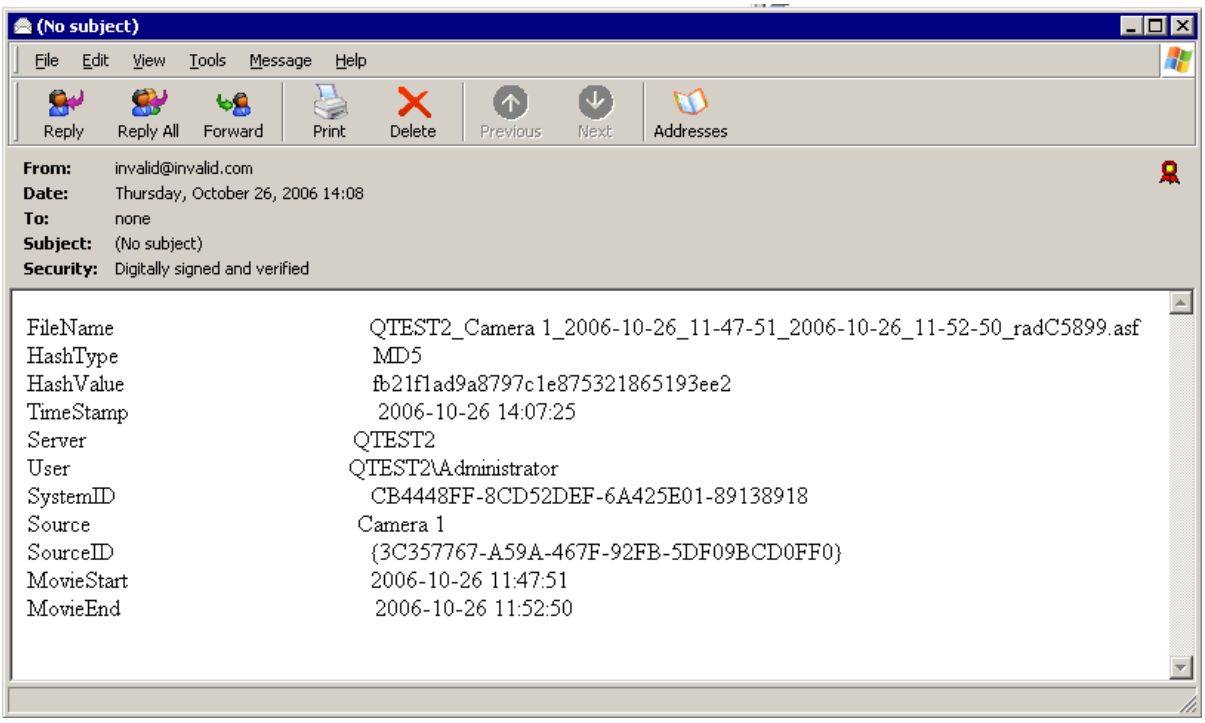

Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
QTEST2 D5CB4ED6-C7AC2C61-AC6795EC-A6138FB9
Windows cannot validate that the certificate is actually from "QTEST2 D5CB4ED6-C7AC2C61-AC6795EC-A6138FB9". You should confirm its origin by contacting "QTEST2 D5CB4ED6-C7AC2C61-AC6795EC-A6138FB9". The following number will assist you in this process:
Thumbprint (sha1): B91DC763 BA4283C4 7FA72B72 C7F49B5C F02C76E6
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

Security Warning Screen

8 Appendix B

You can manually verify the digital signature by using either the .eml or the .p7m format.

- Signatures in .eml format can be viewed by MS Outlook Express. To do that, double click on the .eml file you just saved, Outlook Express opens the signature and you will see the following screen.



Digital Signature Screen

- Signatures in .p7m format can be viewed by a p7mViewer or another relevant viewer (http://www.cryptigo.com). To do that, install the viewer and double click on the .p7m file you just saved. The p7mViewer opens the signature and you will see a screen, which is similar to the one above.

Being able to open a digital signature file and see the information inside implies that it can be decoded (and thus was generated) by the certificate. This means that the signature file itself cannot have been tampered with.

The digital signature generated by Quadrox software contains the following information:

- The filename of the signed movie.
- The signed movie hash type and value. Together, the filename and hash value indisputably link the signature to the movie file.
- The time at which the video was recorded.
- The name of the recorder where the video was recorded and exported.
- The system user that created the movie export.
- The identifier of the recorder, which together with the certificate that

was used proves that the movie file was originally recorded on that particular system.
- The name of the camera that recorded the exported footage.
- The identifier of the camera that recorded the exported footage.
- The start time of the exported footage.
- The end time of the exported footage.

A hash value or a checksum for a file is a short value, something like a fingerprint of the file. This feature can be useful both for comparing the files and their integrity control.

A hash is a mathematically calculated number that uniquely defines the original information. There are always several information strings that have the same hash as a result, but it is infeasible to find a "second original" based only on the hash. If you change a single bit in the original information, the hash will be different. Popular hashes used by the Quadrox software are MD5 and SHA-1.

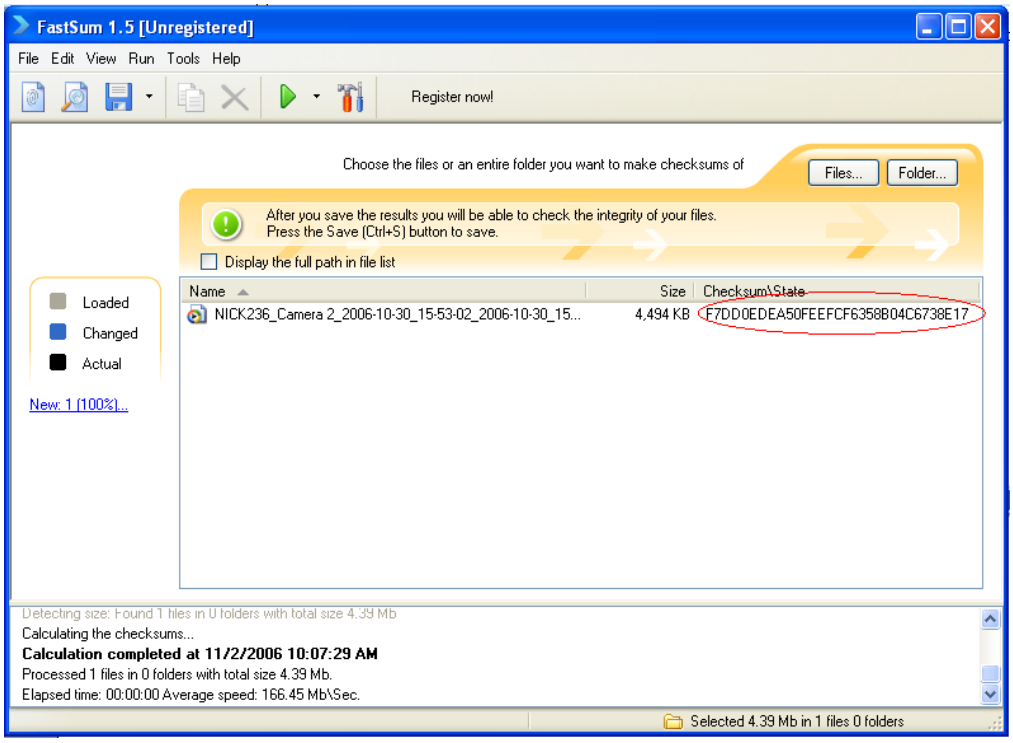
The Hash value can be checked by using the special tools that are built upon the MD5 checksum algorithm which is used worldwide for checking the integrity of the files, for example FastSum application (http://www.fastsum.com).

To calculate the movie's hash value by means of the FastSum application, follow the steps below:

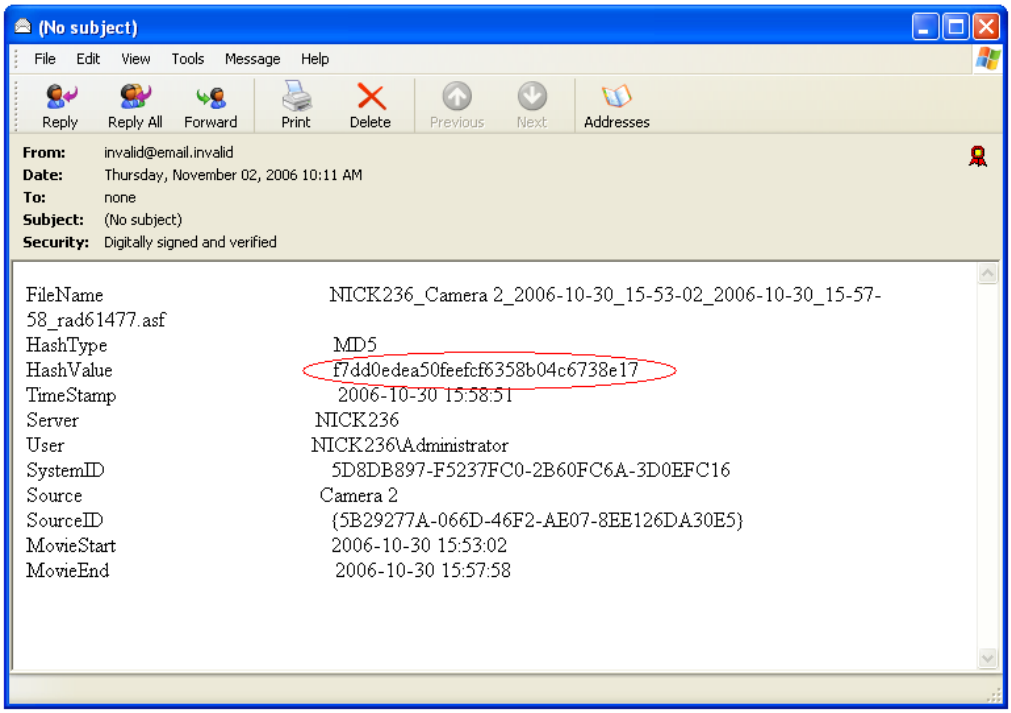
1. Download and install the **FastSum** application by using all the default settings.
2. Right-click on the export file and make the selection as shown on the following screen.

Create Checksum Selection Screen

3. Click the **F9** button in the FastSum screen that appears to begin the calculation.
4. When the checksum is calculated by means of FastSum, compare it with the one from the digital signature.


FastSum 1.5 [Unregistered]
File Edit View Run Tools Help
Register now!
Choose the files or an entire folder you want to make checksums of
Files...
Folder...
After you save the results you will be able to check the integrity of your files.
Press the Save (Ctrl+S) button to save.
Display the full path in file list
Loaded
Changed
Actual
New: 1 [100%]...
Name
Size
Checksum\State
NICK236_Camera 2_2006-10-30_15-53-02_2006-10-30_15...
4,494 KB
F7DD0EDEA50FEEFCF6358B04C6738E17
Calculating the checksums...
Calculation completed at 11/2/2006 10:07:29 AM
Processed 1 files in 0 folders with total size 4.39 Mb.
Elapsed time: 00:00:00 Average speed: 166.45 Mb\Sec.
Selected 4.39 Mb in 1 files 0 folders

FastSum Screen



Digital Signature Screen

If the checksums don't correspond, this means the movie file is not valid and has been changed.

To check the hash value of an exported movie file by means of the FastSum application, follow the steps below:

1. Download and install the **FastSum** application (http://www.fastsum.com).
2. Create an empty text file with **.md5** extension.
3. Edit the file in the following way:

fb21f1ad9a8797c1e875321865193ee2 *QTEST2_Camera 1_2006-10-26_11-47-51_2006-10-26_11-52-50_radC5899.asf

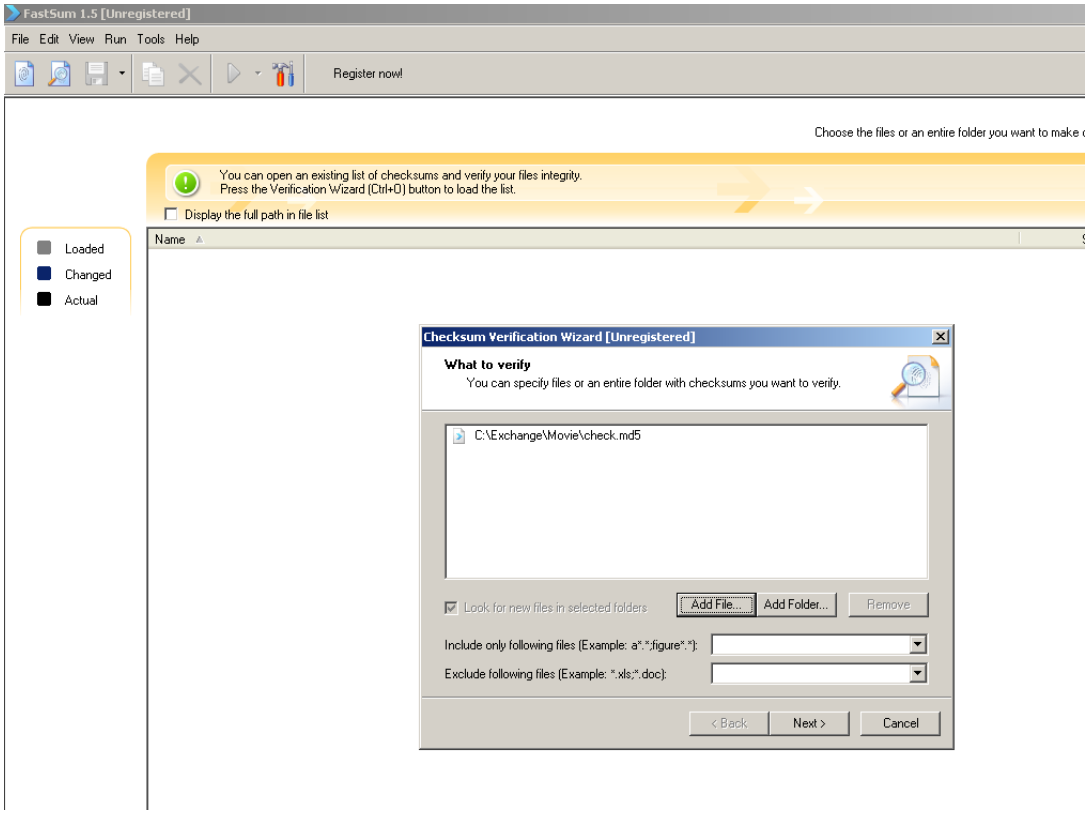
The string above is an example.

Assuming that

fb21f1ad9a8797c1e875321865193ee2 – is the hash value/checksum, which is taken from the digital signature of the exported movie file you want to validate.

QTEST2_Camera 1_2006-10-26_11-47-51_2006-10-26_11-52-50_radC5899.asf – is the name of the exported movie file you want to validate.

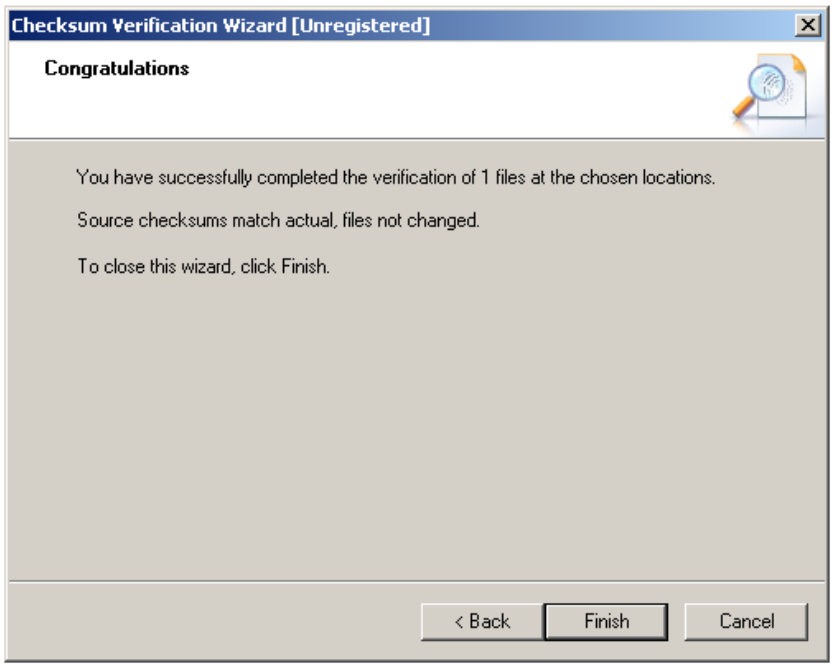
4. Save the edited **.md5** file.
5. Put the saved **.md5** file and export movie file in the same folder.
6. Launch the **FastSum** application and go to **File -> Verification Wizard**.
7. Click **Add File** in the screen that appears and select **.md5** file you created.


FastSum 1.5 [Unregistered]
File Edit View Run Tools Help
Register now!
Choose the files or an entire folder you want to make
You can open an existing list of checksums and verify your files integrity.
Press the Verification Wizard (Ctrl+O) button to load the list.
Display the full path in file list
Name
Loaded
Changed
Actual
Checksum Verification Wizard [Unregistered]
What to verify
You can specify files or an entire folder with checksums you want to verify.
C:\Exchange\Movie\check.md5
Look for new files in selected folders
Add File...
Add Folder...
Remove
Include only following files (Example: a*.*;figure*.*):
Exclude following files (Example: *.xls;*.doc):
< Back
Next >
Cancel

FastSum Application Screen

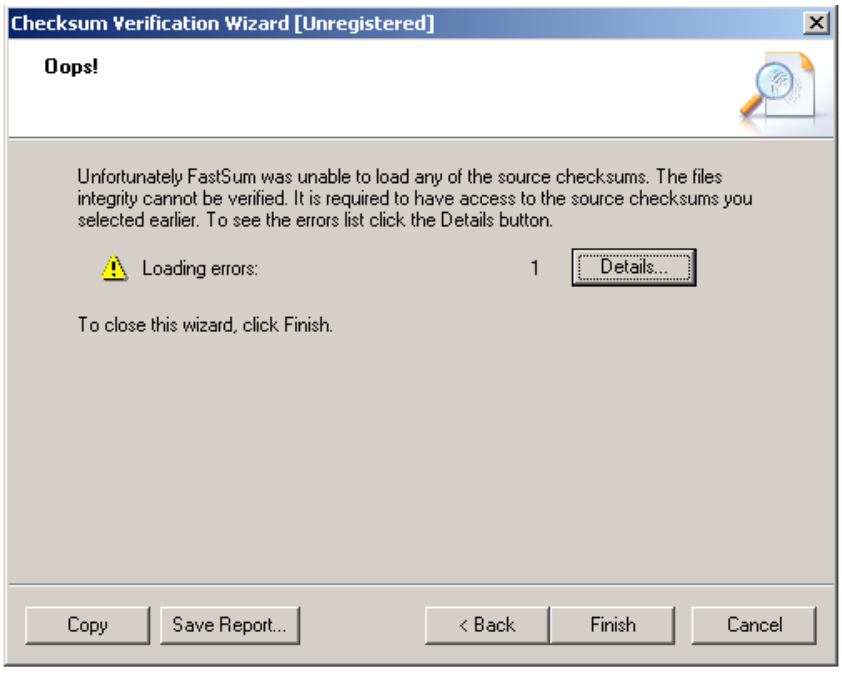
8. Click the **Next** button.

9. If the movie file wasn't changed and the checksum corresponds to the movie file, you will see the following screen:


Checksum Verification Wizard [Unregistered]
Congratulations
You have successfully completed the verification of 1 files at the chosen locations.
Source checksums match actual, files not changed.
To close this wizard, click Finish.
< Back
Finish
Cancel

Checksum Verification Wizard Screen

10. If the checksum doesn't correspond to the movie file, this means that the movie file is not valid and has been changed. You will see a screen denoting such an error:


Checksum Verification Wizard [Unregistered]
Oops!
Unfortunately FastSum was unable to load any of the source checksums. The files integrity cannot be verified. It is required to have access to the source checksums you selected earlier. To see the errors list click the Details button.
Loading errors:
1
Details...
To close this wizard, click Finish.
Copy
Save Report...
< Back
Finish
Cancel

Checksum Verification Wizard Screen

9 Glossary

The terms in this glossary cover topics related to the WebCCTV User's Manual.

A

Activation code – special collection of the characters supplied with the software, used for the software registering.

ActiveX – is a set of technologies from Microsoft providing tools for linking a desktop application to the World Wide Web. Also they are used in the interface and creating other software components.

Activity detection – is a function that enables recording only when movement occurs.

Application – a group of programs that together are used for a specific task such as accounting, financial planning, word processing, games etc.

B

Backup – a copy of a program or data from a computer onto a data-storage medium, usually one that may be removed to safe storage at a distance from the computer; it is used to preserve data for use in the contingency that the original data on the computer may be lost or become unusable.

Browser – is a computer program used for accessing sites or information on a network (as the World Wide Web).

Byte – is the representation of a single character. A sequence of eight bits treated as a single unit, also the smallest addressable unit within the system.

C

Camera Wizard – is a function for facilitation of the camera setting and editing.

Capturing – this option means image recording in a computer-readable form.

Check box – is an interface element that provides parameter or other data selection. When the user clicks a check box to select an option, a V appears in the box.

COM1, COM2 – the names assigned to the serial and communication ports.

Control panel – a collection of the functional buttons. Usually it is arranged at the bottom of the window.

CPU – is an abbreviation for Central Processing Unit. This is the portion of the computer that interprets and executes instructions.

CRT – is the abbreviation for Cathode Ray Tube. This is a vacuum tube in which beams are projected on a fluorescent screen-producing luminous spots. An example is the television set.

Cursor – is a small blinking rectangle or line that indicates the current position on the display screen.

Curtain areas – are areas of constant movement and are classified as not important for surveillance.

D

Data compression – process of reducing the amount of data needed for storage or transmission of a given piece of information (text, graphics, video, sound, etc.), typically by use of encoding techniques.

Default – is the parameter value automatically selected by the system when you or the program does not provide instructions. It is also called a preset value.

Delete – the removing of data from a disk or other data storage device.

Dialog box – an interface element that requires the user to provide further information, such as number of copies to print.

Differential transmission – an option allowing the decrease in the amount of data sent over the network, because only the differences between images are sent over the network when this option is enabled.

Display – CRT, plasma screen, LCD, or other image producing device used to view computer output.

DNS (Domain Name System) – is a database system that translates an IP address into a domain name. For example, a numeric address like 192.168.120.54 can become something like camerasite.com.

Driver – is a program that controls communication between a specific peripheral device and the computer.

Drop-down button (menu) – is a menu of options that appears below the item when the computer user clicks on it.

F

Fan (Cooler) – a device for hardware components cooling.

File – a collection of related information; a file can contain data, programs or both.

Folder – Windows element used to store documents or other folders.

Frame rate – an option used in the recordings setting for defining the number of frames recorded per second per camera.

G

Gigabyte (GB) – is a unit of information equal to one billion (1,073,741,824) bytes or 1024 megabytes.

H

Hard disk – a digital memory device consisting of a flat disk covered with a magnetic coating on which information is stored.

Hardware – the sum of all the physical objects, such as the electrical, mechanical, and electronic devices which comprise a computer system; as, the typical PC hardware suite consists of a mainboard and a number of peripherals such as hard drives and speakers, connected by adapter cards, but the input and output from users occurs mostly through the keyboard and monitor; contrasted with software which are the programs executed by the computer.

I

Icon – a small graphic image displayed on the screen or in the indicator panel. In Windows an icon represents an object that the user can manipulate.

Internet Explorer – Microsoft's free World Wide Web browser for Microsoft Windows and Macintosh.

Image refresh rate – an amount of images the camera sends per one second.

Infrared sensor – is a cable-less communication tool capable of accepting and reacting for infrared signals.

Interface – 1) Hardware and/or software components of a system used specifically to connect one device to another. 2) Physical connection of the one system or device to another for information exchanging. 3) The point of contact between user, the computer and the program.

IO device – equipment used to communicate with the computer and transfer data to and from it.

IP address – a number that uniquely identifies each computer on the Internet or local network (see PMD IO Device also).

IP camera – a camera that has its own IP address and captures, transmits images electronically rather than on film.

J

JPEG – is a standard format of the compression technology (see data compression).

M

Masking – with this feature activated, only images with relevant activity in specified area(s) will be recorded, which increases the recording time significantly.

Megabyte (MB) – is a unit of information equal to one million (1,048,576) bytes or 1024 kilobytes.

MPEG – is a standard format of the compression technology (see data compression).

N

NTSC (National Television Standards Committee or National Television Systems Committee) – the standard television video signal format used in the U.S. and Japan. In Europe the formats most often used are PAL and SECAM.

O

Operating system – is a group of programs that controls the basic operation of a computer. Operating system functions include interpreting programs, creating data files and controlling the transmission and receipt (input/output) of data to and from memory and peripheral devices.

P

PC – abbreviation for Personal Computer.

PAL (Phase Alternate Line or Phase Alternation Line) – the standard for color television broadcast throughout much of Europe, which has good color transmission and sends an analog signal at 625 lines of resolution 25 interlaced frames a second.

Pan Tilt Zoom (PTZ) camera – camera with moveable lens.

Password – a unique string of characters used to identify a specific user. The computer provides various levels of password protection such as user, supervisor, and administrator.

Picolo IO Proxy – equipment for alarm processing.

PMD IO Device – equipment for alarm processing.

Pop-up menu – a list displayed on the computer screen, by which a program provides the user with different options for processing by the program. It usually includes a mechanism, such as pointing by a mouse or selection by arrow keys, to select the desired option from those on the list.

Port – the electrical connection through which the computer sends and receives data to and from devices or other computers. This term means a part of IP logical connection also. For instance: http://192.168.100.1:5000. Where 5000 is a port number.

R

Radio buttons - a group of buttons on the computer screen of which only one can be selected at a time (by clicking on it). Radio buttons are commonly used with interactive forms on World Wide Web pages.

Reboot – resetting a computer without turning it off. There is a special button that allows the rebooting of a WebCCTV server when it is required.

Resolution – the number of pixels per square inch on a computer-generated display. The higher the resolution, the clearer the picture.

S

Sequence time – an option for interval time defining. It is used in some WebCCTV functions.

Server – a computer in a network that is used to provide services (as access to files or shared peripherals or the routing of e-mail) to other computers in the network.

Slider – an interface element that provide the handling and changing of the certain parameter.

Snapshot – an image of a certain video moment.

Software – the set of programs, procedures and related documentation associated with a computer system. Specifically refers to computer programs that direct and control the computer system's activities.

Streaming – an option for activity detection of the cameras that have been watched in live view.

SVHS (Super Video Home System) – a high-quality video format that has higher resolution than normal VHS. It must be played on a videocassette recorder that supports the SVHS format, and to see the sharper image resulting from the higher resolution, it must be played on a high-resolution television set.

System configuration – the specific components in your system (such as the terminal, printer and disk drives) and the settings that define how your system works.

System downloads – a function that allows downloading WebCCTV concerned software.

T

TCP/IP – these two protocols were developed by the U.S. military to allow computers to talk to each other over long distance networks. IP is responsible for moving packets of data between nodes. TCP is responsible for verifying delivery from client to server. Nowadays these two protocols are used in the Internet for providing data transmitting mostly.

TCP Server Port – is used to allow external users to receive alarms, control PTZ cameras, send commands, etc.

U

UDP Streaming Ports – are used to transmit video streams. WebCCTV choose necessary amount of ports from range 4096-4224 and transmit video streams by means of them.

UDP Datagram – is the packet (datagram), on which video stream is divided for proper transmission through the network.

V

VHS (Video Home System) – the standard home videocassette format, which has 1/2" videotape and up to 160 minutes playing time.

Video card – a circuit board fitted to a computer, containing the necessary video memory and other electronics to provide a bitmap display. Adaptors vary in the resolution (number of pixels) and number of colors they can display, and in the refresh rate they support. The monitor attached to the adaptor also limits these parameters. A number of such display standards, e.g. SVGA, have become common and different software requires or supports different sets.

Video memory –an amount of the video card memory.

Virtual Patrol – this function allows camera inspecting of the different sites at the given times. It allows active 24 hour monitoring of a big area with only one camera.

W

Window – a portion of the screen that can display its own application or document. Often used to mean a Microsoft Windows window.

Windows XP – an operating system based on the windows effect. Created by Microsoft Corporation.